CR-137730

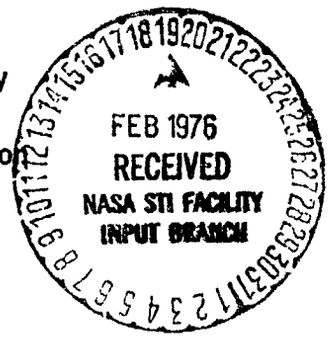
available to the Public

FAILURE DETECTION AND ISOLATION INVESTIGATION FOR STRAPDOWN SKEW REDUNDANT TETRAD LASER GYRO INERTIAL SENSOR ARRAYS

By A. J. Eberlein and T. G. Lahn

Prepared under Contract No. NAS2-8065 by

HONEYWELL INC.
Government and Aeronautical Products Division
Minneapolis, Minnesota 55413



For

AMES RESEARCH CENTER
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

CONTENTS

CONTENTS (Continued)

CONTENTS (Continued)

CONTENTS (Concluded)

FIGURES

FIGURES (Concluded)

TABLES

LIST OF SYMBOLS

A_C	Accelerometer self-test deficiency
A_F	Accelerometer failure rate
A/D	Analog-to-digital conversion
C_F	Computer failure rate
C_C	Computer self-test deficiency
CCW	Counter clockwise
cm	Centimeter
CPU	Central processor unit
CW	Clockwise
D/A	Digital-to-analog conversion
DCM	Dynamic computation monitor
E_m	Estimated monitor effectiveness
FO	Fail-operative
FS	Fail-safe
G_C	Gyro self-test deficiency
G_F	Gyro failure rate
I_1	Current in laser gyro leg 1
I_2	Current in laser gyro leg 2
INC	Inertial navigation channel
I/O	Input/output
I_t	Total current ($I_1 + I_2$)
MTBF	Mean time between failure
MTBLF	Mean time between loss of function
n	Number

P_{CCW}	Counter-clockwise pulse
P_A	Probability of an inoperative system
P_{CF}	Probability of a potentially catastrophic failure
P_{DF}	Probability of a detected failure
P_{CW}	Clockwise pulse
P_{FO}	Probability of a fail-operative condition
P_{FS}	Probability of a fail-safe condition
P_{IF}	Probability of an indicator failure
P_{UF}	Probability of an undetected failure
PZT	Piezoelectric
t	Time
WTD	Watchdog timer
λ	Failure rate (%/1000 hours)
δ	Error

FAILURE DETECTION AND ISOLATION INVESTIGATION FOR STRAPDOWN SKEW REDUNDANT TETRAD LASER GYRO INERTIAL SENSOR ARRAYS

By A.J. Eberlein and T.G. Lahn
Honeywell Inc.

SUMMARY

A study was performed to determine the degree to which flight-critical failures in a strapdown laser gyro tetrad sensor assembly can be isolated in short-haul aircraft after a failure occurrence has been detected by the skewed sensor failure-detection voting logic. Also investigated was the degree to which a failure in the tetrad computer can be detected and isolated at the computer level, assuming a dual-redundant computer configuration.

The tetrad system was mechanized with two two-axis inertial navigation channels (INCs), each containing two gyro/accelerometer axes, computer, control circuitry and input/output circuitry. Gyro/accelerometer data is crossfed between the two INCs to enable each computer to independently perform the navigation task. Computer calculations are synchronized between the computers so that calculated quantities are identical and may be compared.

No way was found to guarantee complete fail-operational/fail-safe performance from a tetrad with redundant computers. Fail-safe performance (identification of the first failure) can be accomplished with a probability approaching 100% of the time, while fail-operational performance (identification and isolation of the first failure) can be achieved 93 to 96% of the time. During those times when the system operates satisfactorily after the first failure (first failure has been identified and isolated), fail-safe performance (identification of the second failure) can be accomplished 93 to 96% of the time.

SECTION 1
INTRODUCTION

This report documents the results of a study performed by Honeywell Inc. investigating laser gyro self-test capability and computer self-test concepts as applicable to a strapdown tetrad inertial navigation system. Prior to this study the fail-operational/fail-safe characteristics of a tetrad INS mechanized with laser gyros had not been investigated.

The study was initiated by NASA Ames Research Laboratory to determine the performance viability of a tetrad strapdown inertial navigation system against a fail-operational/fail-safe criterion. A tetrad consisting of two two-axis inertial navigation channels (INCs) was configured as a reference, with the main thrust of the study aimed at gyro self-test capability and computer fault isolation.

Section 2 describes the tetrad configuration chosen as a reference and describes the relationship between the two two-axis INCs. Section 3 discusses tetrad system redundancy management concepts as applicable to the gyros and computers. Included in this section are general reliability considerations and two alternate dual-computer configurations. Section 4 describes the functional areas of the laser gyro along with a reliability analysis of each functional area. The impact of a failure in each functional area is assessed and BIT circuitry identified to detect the failure. A probability of failure detection is arrived at for each functional area within the laser gyro. Section 5 describes failure detection and isolation techniques that can be used to self test either of the dual computers. A qualitative evaluation of the self-test effectiveness is also provided so that the feasibility of the concept can be evaluated. Section 6 assesses the impact on short-haul aircraft safety of flight of using the tetrad gyros for stability augmentation, attitude reference and navigation.

SECTION 2
TETRAD SYSTEM DESCRIPTION

The tetrad skewed sensor array represents the simplest form of gyro redundancy that may be mechanized into a strapdown navigation system. A tetrad array combined with a dual-redundant computer configuration was used to mechanize the tetrad inertial navigation system investigated in this study.

Skewed sensor redundancy is a technique that enables a single inertial sensor (gyro or accelerometer) to replace any failed sensor regardless of its input axis orientation. The concept is to mount the sensors such that their input axes are nonorthogonal (skewed) relative to one another, with any set of three input axes nonplanar. With this arrangement, any set of three sensor outputs can be used to derive (in the system computer) the equivalent output of an orthogonal sensor triad. Thus, four skewed sensors would be capable of generating complete three-axis orthogonal output data with up to one sensor failure, and five skewed sensors would be capable of tolerating two failures. In a conventional redundancy approach, two sets of orthogonal triads (i.e., six sensors) would have the same redundancy capability as four skewed sensors. The hardware savings is substantial with the skewed approach as the redundancy requirement increases.

In the strapdown approach, the inertial sensor triad (gyros and accelerometers) are mounted directly to the airframe. Both the gyro and accelerometer outputs are directed to the system computer. The computer processes the gyro data to continuously determine aircraft attitude relative to earth-referenced coordinates. The attitude data is used with the aircraft-mounted accelerometer signals to compute the equivalent acceleration data in the earth-referenced coordinate frame. Thus, the computer analytically simulates the function of the gimbal assembly in the gimbaled approach.

The remainder of the computation to determine aircraft velocity, position, and reference torquing commands is identical to the gimbaled approach. The emergence of the strapdown system as a more practical and cost-effective system rests on the development of digital computers that are relatively inexpensive and that have the computational speeds necessary to perform the strapdown navigation computations rapidly.

Figure 1 is a block diagram showing the general configuration of the tetrad navigation system which consists of two identical two-axis inertial navigation channels. The two angular rate and acceleration signals from each two-axis sensor array are sent to each computer. The computer computational frames are synchronized through the use of a 40-msec clock interchange, while the data crossfeed permits each computer to compare its output with that of its counterpart (see Appendix A).

Other computer inputs generally include an altitude signal, mode control and latitude/longitude initialization data for the inertial computations from the aircraft control panel. Outputs from each computer, in general, are a-c, d-c, digital, and discrete outputs to the other aircraft systems and displays.

The orientation of the input axes of one of the gyro/accelerometer sets in a two-axis inertial navigation channel is shown in Figure 2(a) and is parallel to the long axis of the box (normal to the front face). The second gyro/accelerometer set is mounted with input axes perpendicular to the first set but skewed 54.7 degrees (nonorthogonal) relative to the base. The two two-axis inertial navigation channels are mounted to a common base, which is part of the aircraft rack structure, in precision alignment such that the long axes of the boxes are skewed relative to one another. This mounting arrangement is shown in Figure 2(b).

With the two-axis INCs oriented this way, the gyro/accelerometer sets become aligned relative to one another such that the input axes of the four sensors (tetrad) are noncoplanar (i.e., they do not lie in a single plane).

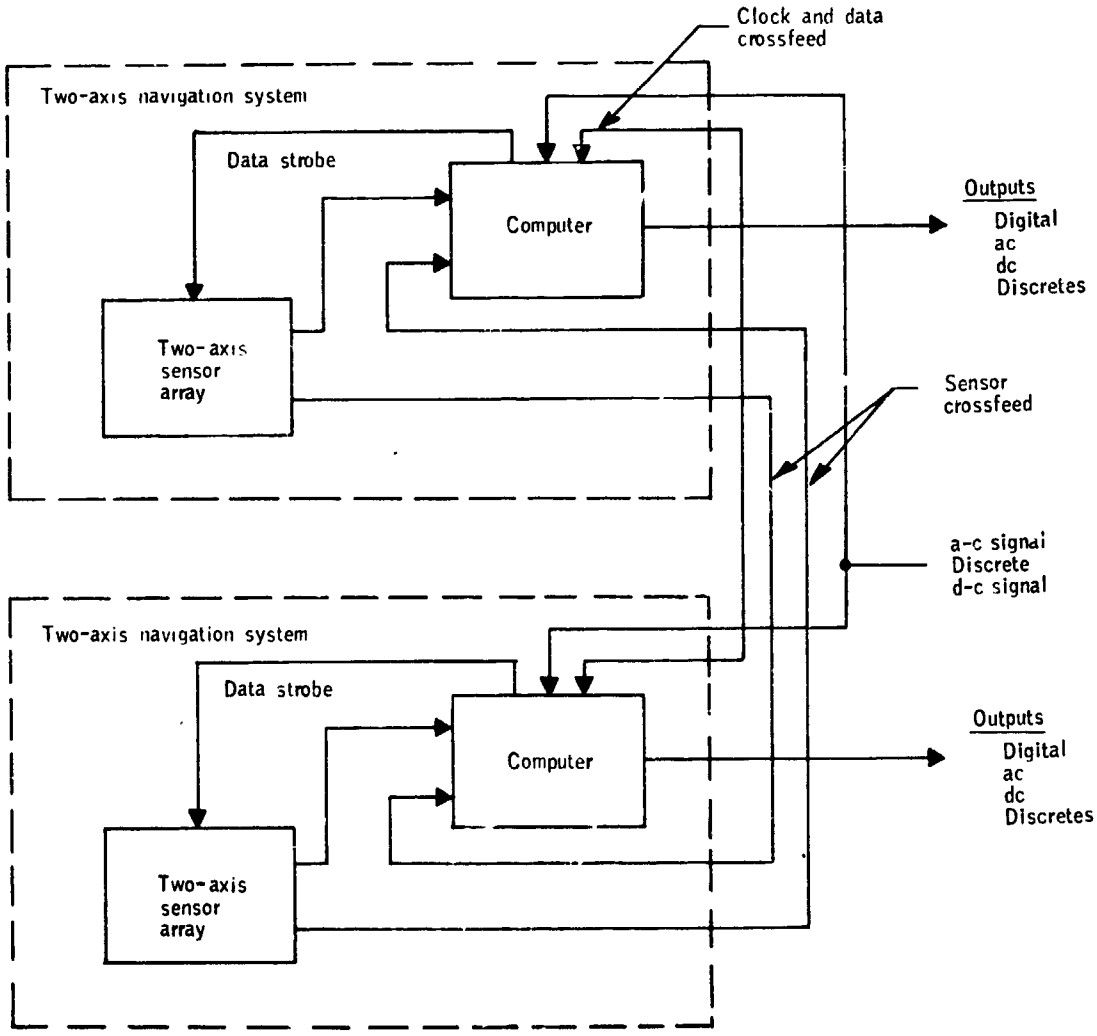


Figure 1. - Tetrad navigation system

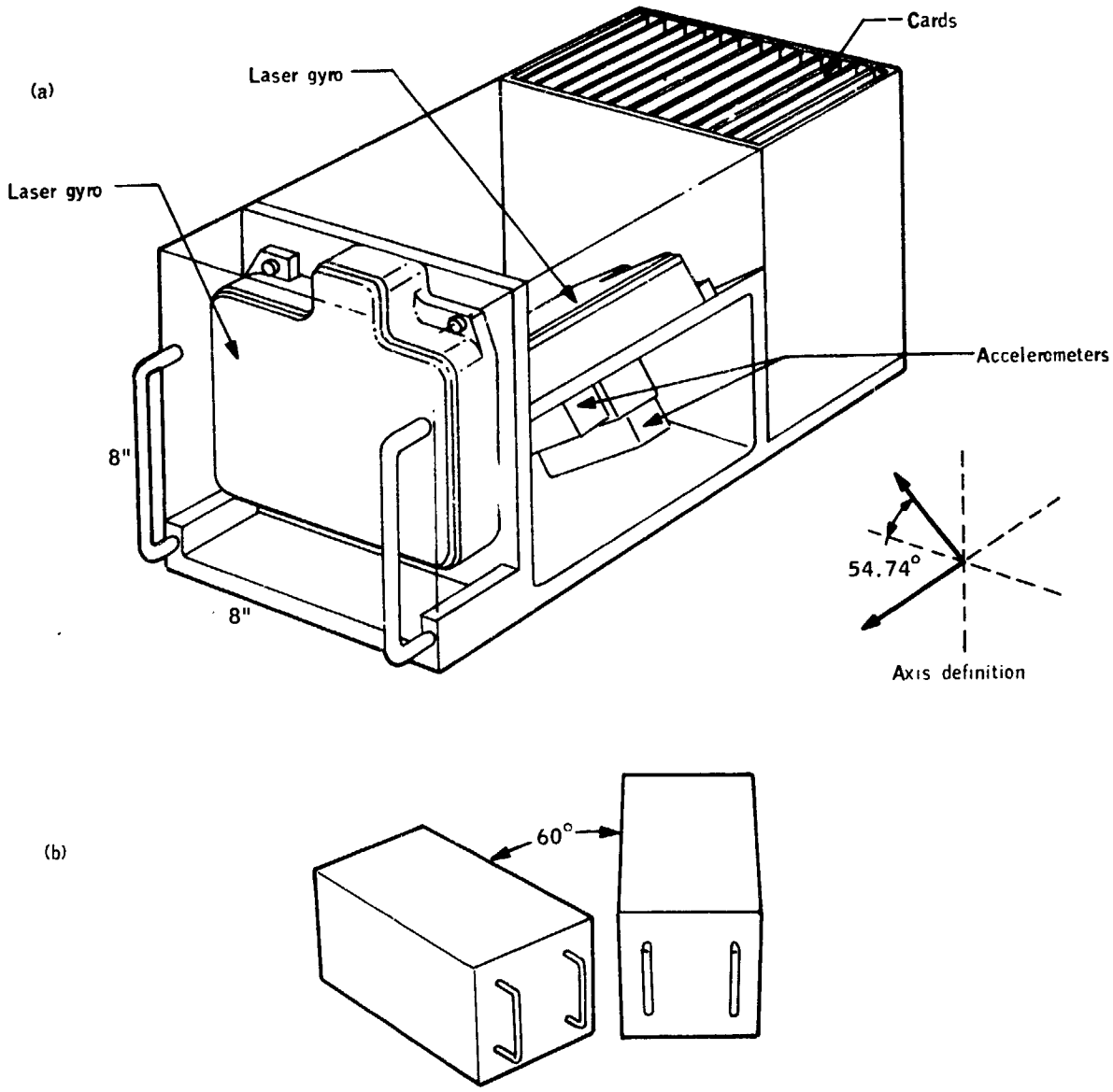


Figure 2. - Tetrad hardware

Under these conditions, software routines in the computer can operate on the tetrad signals to analytically compute the equivalent roll, pitch, and yaw axis rate/acceleration data for computer operations. In addition, three of the four tetrad gyro/accelerometer signals can be combined to analytically derive what the fourth sensor set is measuring. If the derived signals are unequal to the fourth set output (within prescribed tolerances), a failure has occurred in one of the tetrad sensors.

Figure 3 illustrates the inertial computations in the system computers, showing the inertial calculations data flow. The computer first compensates the input data from the two-axis skewed gyro/accelerometer sets for known systematic errors in each instrument such as bias, scale factor, and misalignment. The compensated skewed gyro/accelerometer signals are then compared in the skewed voting algorithms for failure detection and computation of equivalent three-axis orthogonal axis data (roll, pitch yaw axis rate and acceleration), assuming no failure is indicated. Appendix B provides the derivation of a representative set of skewed redundancy gyro voting equations and skew-to-orthogonal transformation equations that would be programmed into the system computer. Skewed accelerometer equations would be similar to those for the gyros in Appendix B.

The roll/pitch/yaw angular rate derived from the skewed gyro voting logic is then used in a three-axis attitude integration algorithm to compute the attitude of the aircraft (more specifically, the accelerometer assembly) relative to local vertical/azimuth coordinates. The angular rate of the aircraft over the surface of the earth (due to earth's rotation and aircraft velocity) is included in this computation to account for the rotation rate of the local vertical.

The aircraft attitude data is used to resolve the roll/pitch/yaw aircraft axis acceleration vector data from the skewed accelerometer voting logic into the local vertical/azimuth coordinate frame. The computed horizontal/vertical acceleration components are then integrated in an inertial velocity/position computation algorithm to calculate aircraft horizontal velocity and

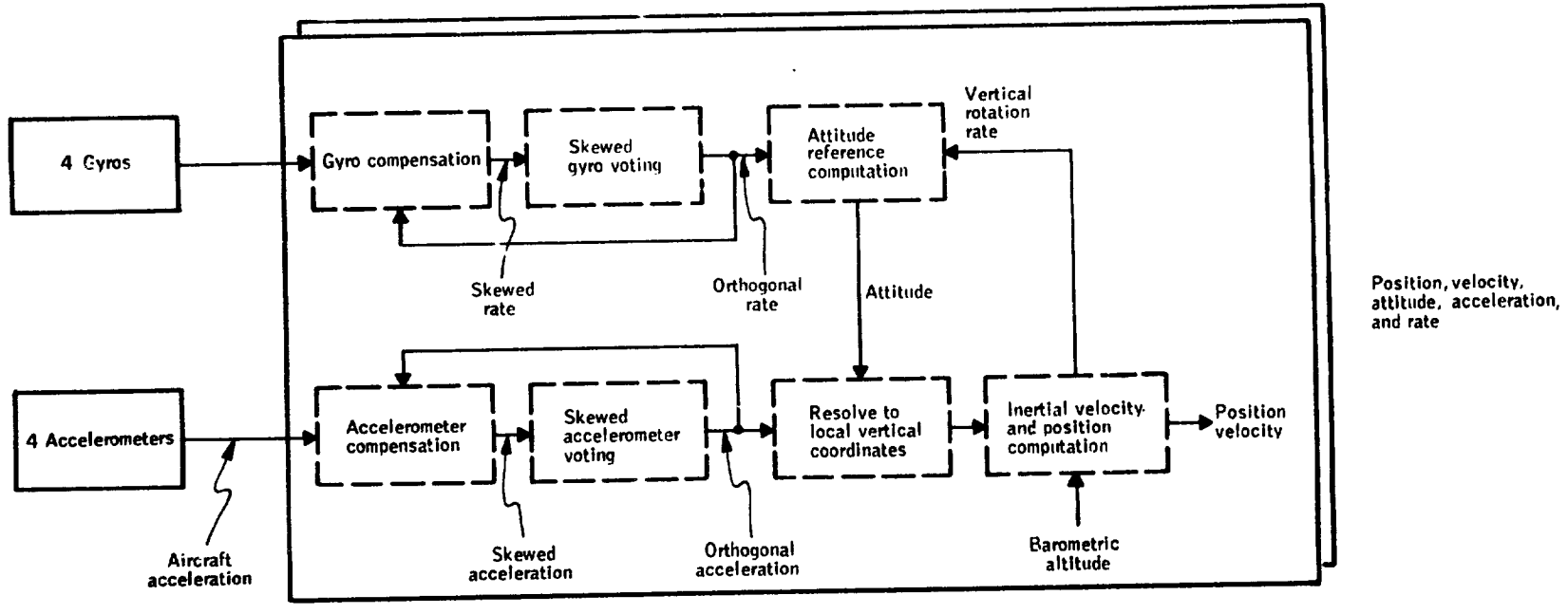


Figure 3. - Strapdown skewed inertial computation

latitude/longitude position. Barometric altitude is used in the inertial computation to stabilize the vertical channel.

Figure 4 shows signal flow through the tetrad. The sensor signals are crossfed to the control and holding circuitry of each two-axis navigation system. The sensor information is stored in memory until it is subsequently used to calculate the required outputs.

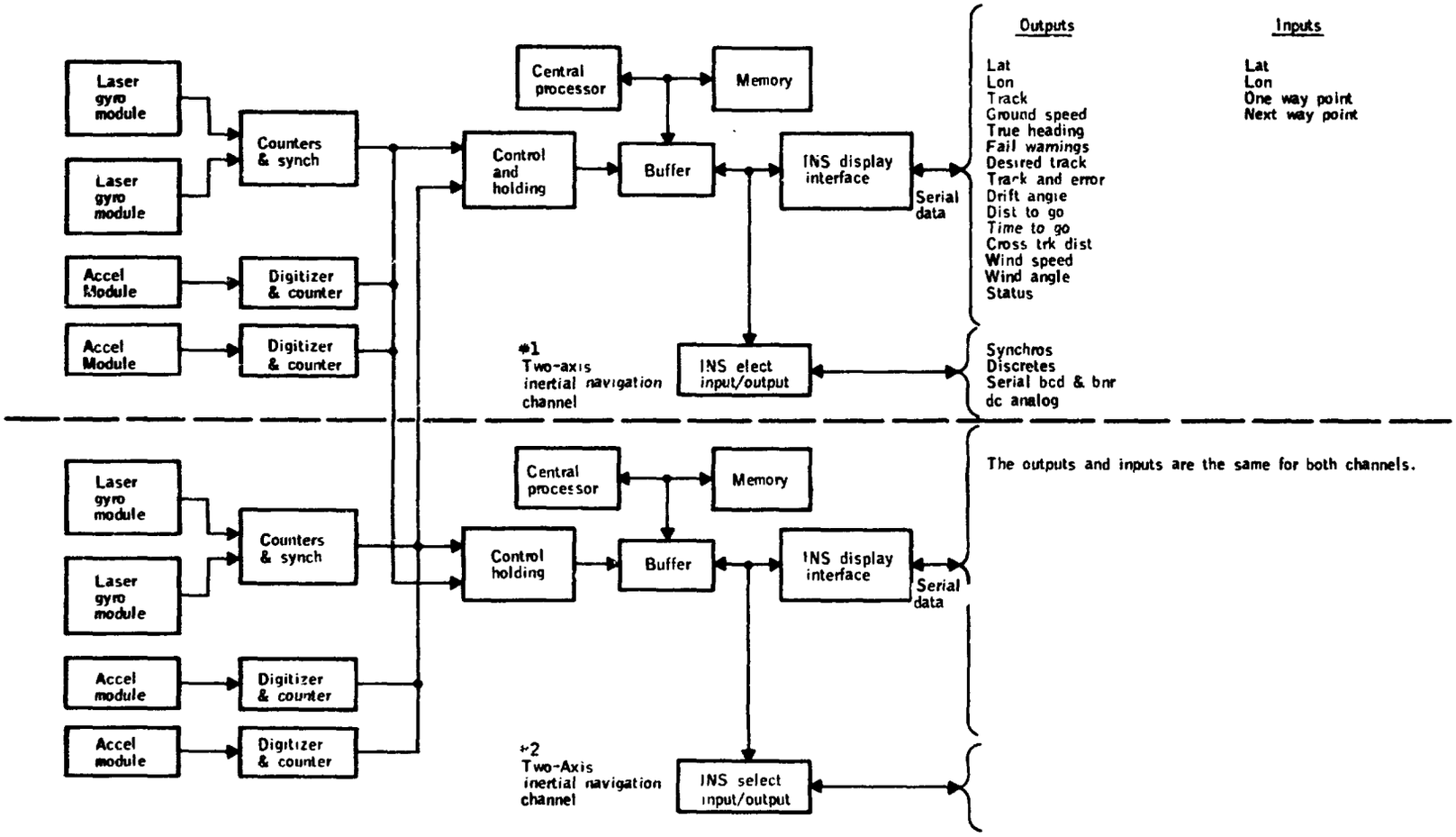


Figure 4. - Tetrad block diagram

SECTION 3
SYSTEM REDUNDANCY MANAGEMENT CONCEPTS

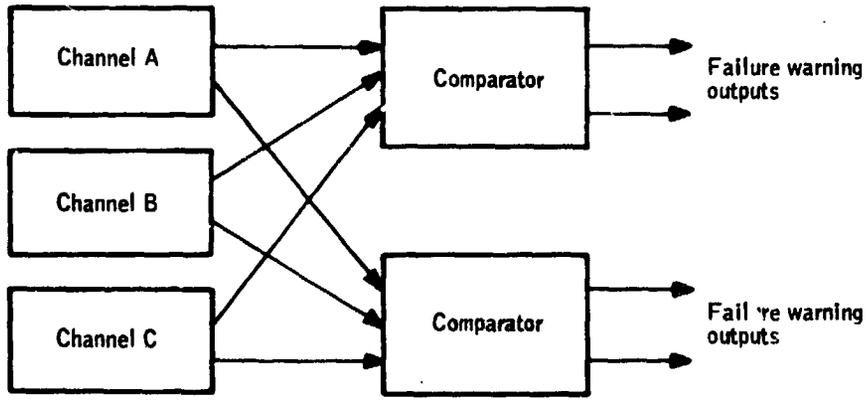
General Reliability Considerations

Past analog systems have relied primarily on the use of additional components (hardware redundancy) to meet system fault specifications (i.e., fail-operational/fail-safe, etc.). When digital systems are considered, various combinations of three types of redundancy can be used -- additional programming for a self check (software redundancy); repetition of calculations or similar calculations for self check (time redundancy); and use of additional components for cross checking (hardware redundancy). Each of these three types of redundancy has its advantages and disadvantages and can be applied in varied degrees depending upon the requirements and philosophy used in the system design.

Computational failures. - Both analog and digital systems can have either transient or permanent faults. However, because of the binary nature of the digital computer, its errors result in logic faults (for example, a "1" is in a specific bit instead of a "0"). Transient and permanent faults are caused by component failures, intermittent malfunctions, and external interference during computation. Most faults will cause an error in the program being executed by the computer -- either an instruction is not executed correctly, or an incorrect result is computed. Faults can cause either or both instruction and result errors. The exact nature of the fault depends on the nature of the component failure.

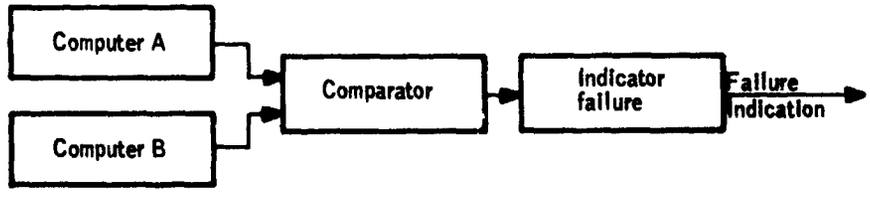
For example, component failures in certain areas of memory or I/O could result in a single bad value or output whereas other component failures in more critical points could result in a completely inoperative computer.

Hardware redundancy. - The use of identical multiple circuits or channels is the most common form of redundancy in modern analog systems:



A triple-channel approach to system redundancy has been used traditionally when fail-operational/fail-safe performance has been required. Flight safety of the above system basically reduces to providing fail-safe operation on any two channels.

The reliability model for a dual-channel fail-safe computer is shown below:



$$P_{CF} = (\quad \cdot P_{IF}) + P_{UF}$$

where

P_{CF} = probability of a potentially catastrophic failure

P_{DF} = probability of a detected failure

P_{IF} = probability of an indicator failure

P_{UF} = probability of an undetected failure

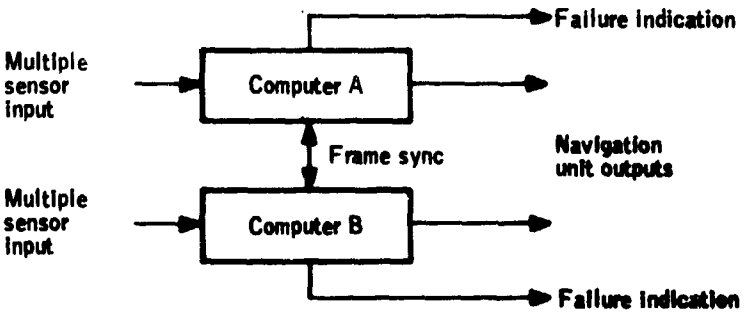
NOTE: INS failures may or may not have the potential for causing a catastrophic condition to exist in the aircraft. The classification of failures is a function of many variables such as flight conditions, navigation mode, effect on flight controls and instruments, etc. In this report a conservative approach is taken relative to failures by assuming that all failures are potential catastrophic failures if they are not detected.

The failing indicator must be designed so that the probability of it failing to respond is very small and the safety problem reduces to: $P_{CF} \cong P_{UF}$ where $(P_{DF} \cdot P_{IF}) \ll P_{UF}$. The probability of a potentially catastrophic condition (P_{CF}) is then approximately equal to the probability of an undetected failure in the computer.

The system is as good as its failure detection capability. For a dual-channel comparison-monitored system, the failure detection is performed by the comparator. Therefore, the system is as safe as the comparator.

To assess the safety of a comparator requires a failure mode and effects analysis on all parts that can affect flight safety. For a comparator these include: the comparator design and circuits plus trip levels and any common elements of the two systems to be compared. A detailed analysis need only be performed on these items to acquire a high confidence in the system safety. Parts counts are low, modes are straightforward, and common elements are easy to identify.

Fail-safe computer approach. - The basic dual-redundant self-check computer configuration (see below) investigated in this study can provide fail-operational/fail-safe capability to the extent that fail-safe operation can be mechanized into a single-channel computer.



The reliability model for the "fail-safe" single computer is shown below.

$$P_{CF} = (P_{DF} \cdot P_{IF}) + P_{UF}$$

where

P_{CF} = probability of a potentially catastrophic failure

P_{DF} = probability of a detected failure

P_{IF} = probability of an indicator failure

P_{UF} = probability of an undetected failure

For a high-reliability system, the failure indicator must be designed so that the probability of the failure indicator failing to respond is very small:

$$P_{CF} \cong P_{UF}$$

where $(P_{DF} \cdot P_{IF}) \ll P_{UF}$. The probability of a potentially catastrophic failure (P_{CF}) is approximately equal to the probability of an undetected failure in the computer.

This simply shows that the system is as good as its failure detection capability. For a single-channel system, failure detection is predominately self-test. Therefore, the system is as safe as its self-test, and significant engineering effort is required in the design of the self-test.

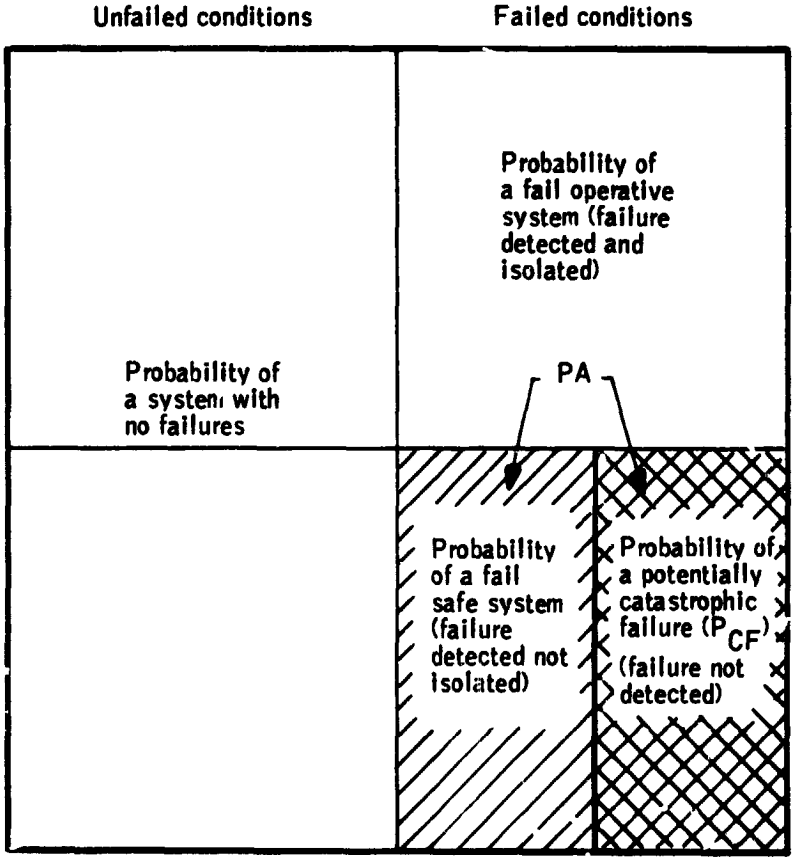
To determine the safety level of a flight system requires failure modes and effects analysis on all parts that can affect flight safety. For a single-channel computer dependent on self-test, these modes include: the processor, memory, BIT circuits, I/O, etc. Once all modes are identified, they can be evaluated to determine if they will be detected. A detailed analysis on a major portion of the system is required to gain any confidence in the self-test system. In general, any failure mode that can be identified can be detected; but, have all modes been defined? Parts counts are high, and it is especially difficult to identify all of the conditional failure modes. Latent failures are always a potential problem.

Reliability design acceptance criteria. - Figure 5 represents the universe of system probabilities, relative to operating status, that are used in this report.

The probability of a failure is the Σ of the λ t's of all the system parts, while the probability of a system with no failures is determined by subtracting the Σ of the λ t's from 1.

The probability of potentially catastrophic failures (P_{CF}) and the probability for an inoperative system (P_A) may be used as a basic design acceptance criteria for redundant systems. The probability of an inoperative system includes the probability of a fail-safe system failure and probability of a potentially catastrophic failure.

The probability of a fail-operative system can be determined by subtracting P_A from the Σ of the λt's for the system. The probability of a fail-safe system can be determined by subtracting P_{CF} from P_A.



P_A = Probability of an inoperative system equals probability of a fail safe system + probability of a potentially critical failure

Figure 5. - System probabilities

Tetrad Sensor/Dual-Computer Redundancy Management Concept

The tetrad sensor/dual-computer redundancy management concept investigated in this study is shown in Figure 6. In this concept, the tetrad sensor assemblies feed all sensor signals and sensor validity signals to both computers. Each computer then performs sensor monitoring and signal selection in the event of a failure. This sensor monitoring in the computer is performed so that even if the sensor self-test is inconclusive, the computers can detect and disengage the system for a first sensor failure.

The selected sensor signals are used to perform the required navigation computations. The outputs of these computations are fed by I/O devices to the output and failure warning circuits. Sensors are tested by a combination of self-test and comparison monitoring by the dual computers. The comparison monitoring ensures fail-safe operation after a first failure. If the sensor self-test is conclusive and the failure can be isolated to a particular sensor, fail-operational performance is achieved using the remaining three sensors. For any subsequent failure, sensor self-test is necessary for safe disengagement. The failure diagrams for the sensors are included in the following computer configuration discussions. The computer self-test also feeds these output and warning circuits.

If a failure is detected by the self-test, a failure will be indicated, and outputs may be inhibited. The basic concept may be used with or without signal comparison of the dual computer. The following subsection discusses dual-computer configuration without output comparison.

Dual-channel computers without output comparison.- Figure 7 shows the failure diagram for a dual-channel computer configuration that relies completely on self-test for computer failure detection. This diagram illustrates the system status for various failure situations, including the fail-operate conditions, the fail-safe disengage conditions and the potentially catastrophic conditions.

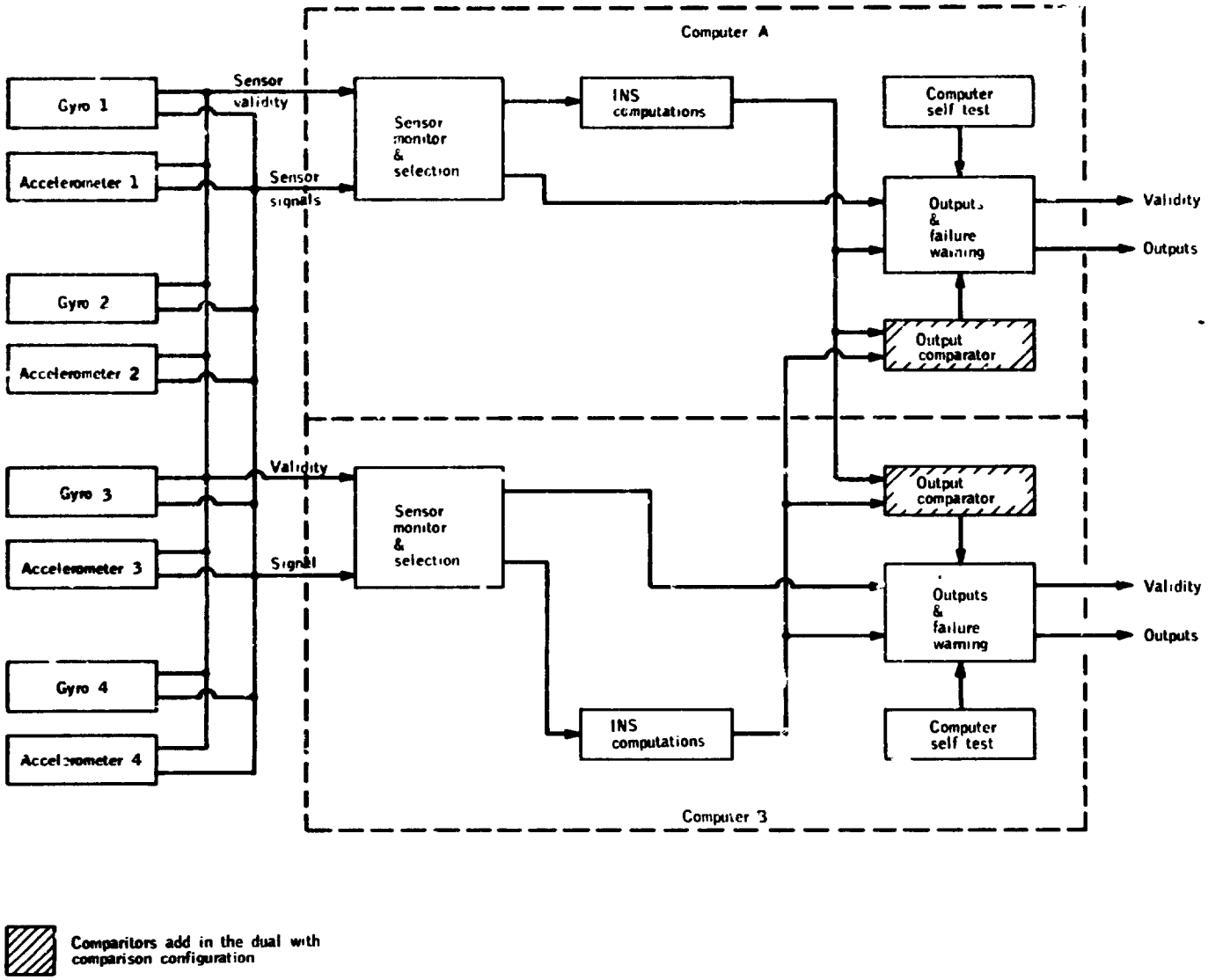
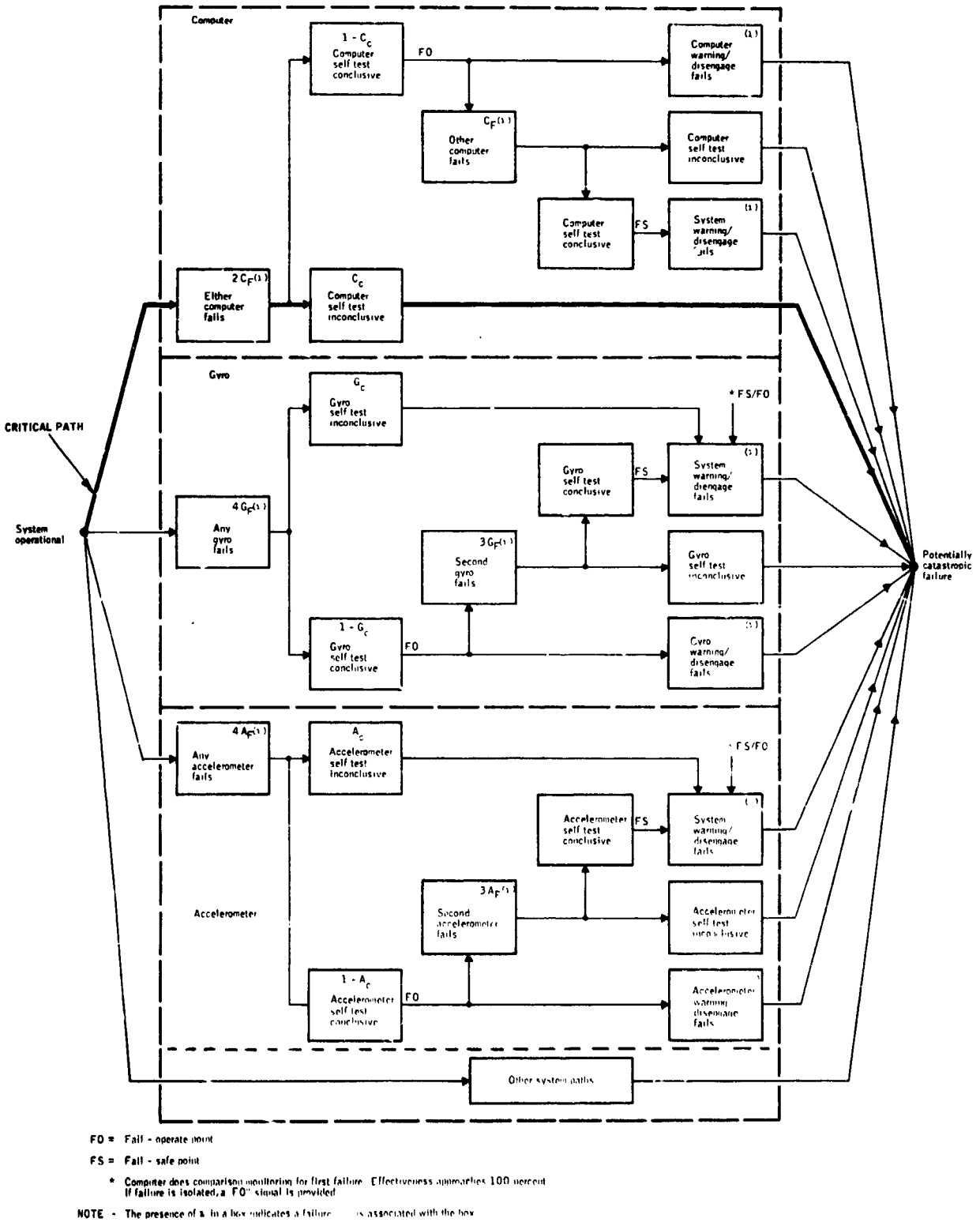


Figure 6. - Tetrad sensor/dual-computer redundancy management concept



FO = Fail - operate point

FS = Fail - safe point

* Computer does comparison monitoring for first failure. Effectiveness approaches 100 percent. If failure is isolated, a "FO" signal is provided.

NOTE - The presence of a ▲ in a box indicates a failure ... is associated with the box.

Figure 7. - Dual-channel computer failure diagram

The fail-operate points are shown by "FO" on Figure 7. These points are found after the first self-test-conclusive box and may be located by following a path (left to right) which includes a single failure and a self-test-conclusive box. The "FO" points means that the failure has been detected and isolated, thus permitting the system to remain operative. A warning light is activated in the cockpit indicating a failure has occurred, but the system remains operative.

The fail-safe points are shown by a "FS" on Figure 7 and mean that a failure has been detected but not isolated. These points are located after the self-test-conclusive box associated with the second failure. A warning light is activated in the cockpit indicating a failure has occurred and that the system can no longer be relied upon and has been automatically disengaged or should be manually disengaged.

A potentially catastrophic failure point is shown in the right side of Figure 7; it may be reached by many paths originating from the point labeled "system operational." The dark line entitled "critical path" on Figure 7 is the dominant failure mode for the configuration where the system is mechanized with two computers which rely on individual self-test for computer failure detection. For this configuration, the P_{CF} can be approximated by considering only the critical failure path through the computer because the probability of a failure in the other paths is several orders of magnitude smaller. Using the procedure in Appendix D and eliminating insignificant terms, the P_{CF} equation from Figure 7 reduces to:

$$P_{CF} = 2\, C_F \cdot C_c \cdot t$$

where

C_F = computer failure rate/hour

C_c = computer test deficiency

t = mission time in hours

This configuration has practical limitations because the computer self-test effectiveness completely dominates the P_{CF} value. Figure 8 shows the overall computer self-test deficiency as a function of the required total failure probability per flight hour (a plot of the previously derived P_{CF} equation for a given C_F). If a P_{CF} of less than 10^{-6} is required, the self-test effectiveness has to be better than 99.9%. (Conversely, the overall computer self-test deficiency has to be less than .001.) Self-test effectiveness approaching this level requires very extensive FMEA analysis.

The following failure rates have been estimated in order to show a calculation of P_{CF} applicable to the critical path shown in Figure 7:

Computer

1 processor at 2.7%/1000 hr	2.7
3 memory cards at 2.0%/1000 hr/card	6.0
12 computer cards at 1.0%/1000 hr/card	12.0

$$C_F \approx 2.1 \cdot 10^{-4} \text{ failures/hr}$$

Computer test deficiency $C = 0.05$

$$\frac{P_{CF}}{t} = 2\, C_F \cdot C_c = \text{failures/hr}$$

$$= 2 \cdot 2.1 \cdot 10^{-4} \cdot .05$$

$$= 2.1 \cdot 10^{-5}$$

The probability of an inoperative system (P_A) due to a computer or sensor failure can be determined from Figure 9 by summing the parallel paths leading to an inoperative system. This results in the following equation (using Appendix D):

$$P_A = \left[2\, C_F C_C + \frac{2}{2!}\, C_F{}^2\, (1 - C_c) + 4\, G_F G_C + \frac{12}{2!}\, G_F{}^2\, (1 - G_C) + 4\, A_F A_C + \frac{12}{2!}\, A_F{}^2\, (1 - A_c)\right] t$$

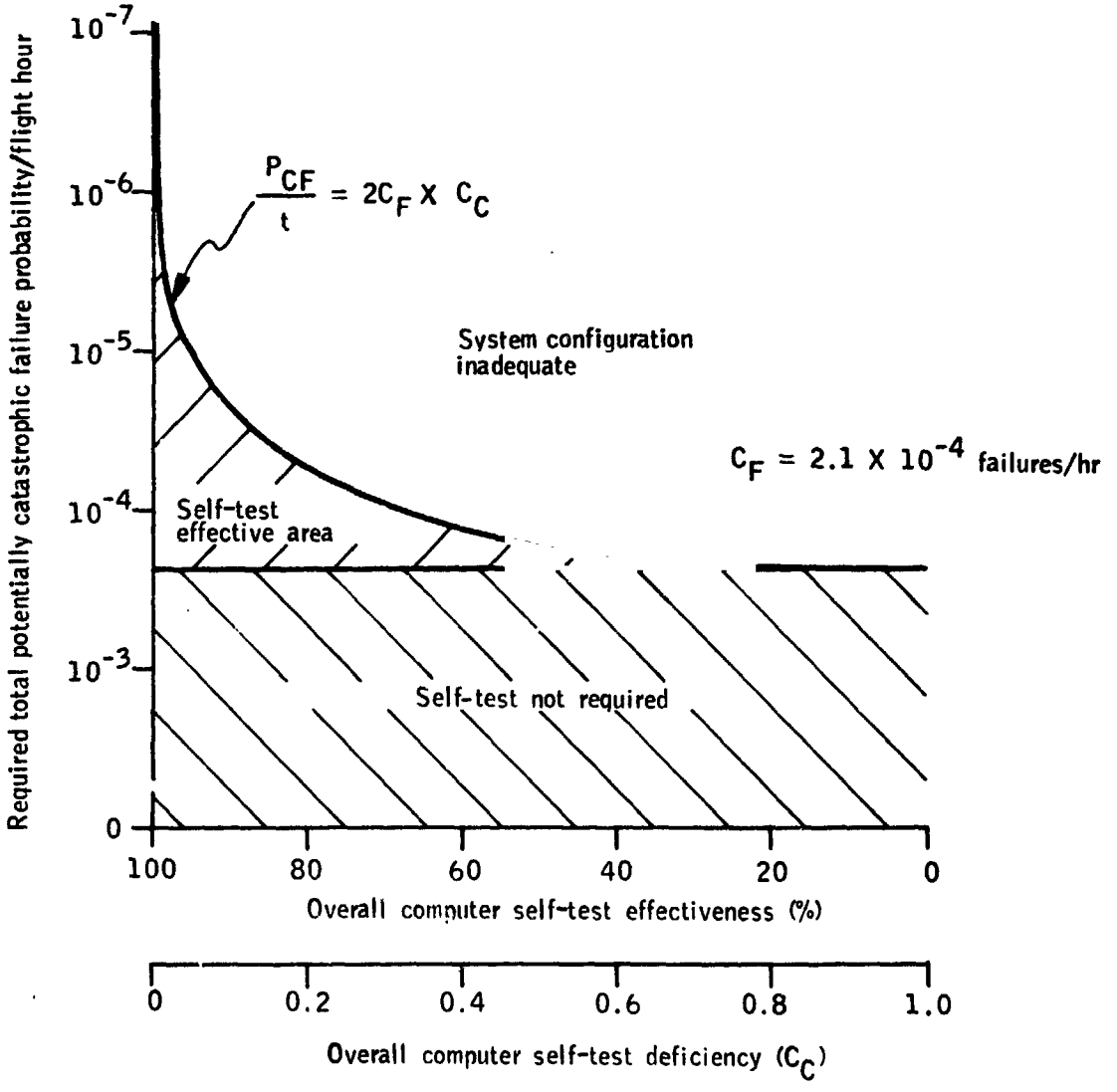


Figure 8. - Effect of self-test on flight safety for a dual-computer configuration

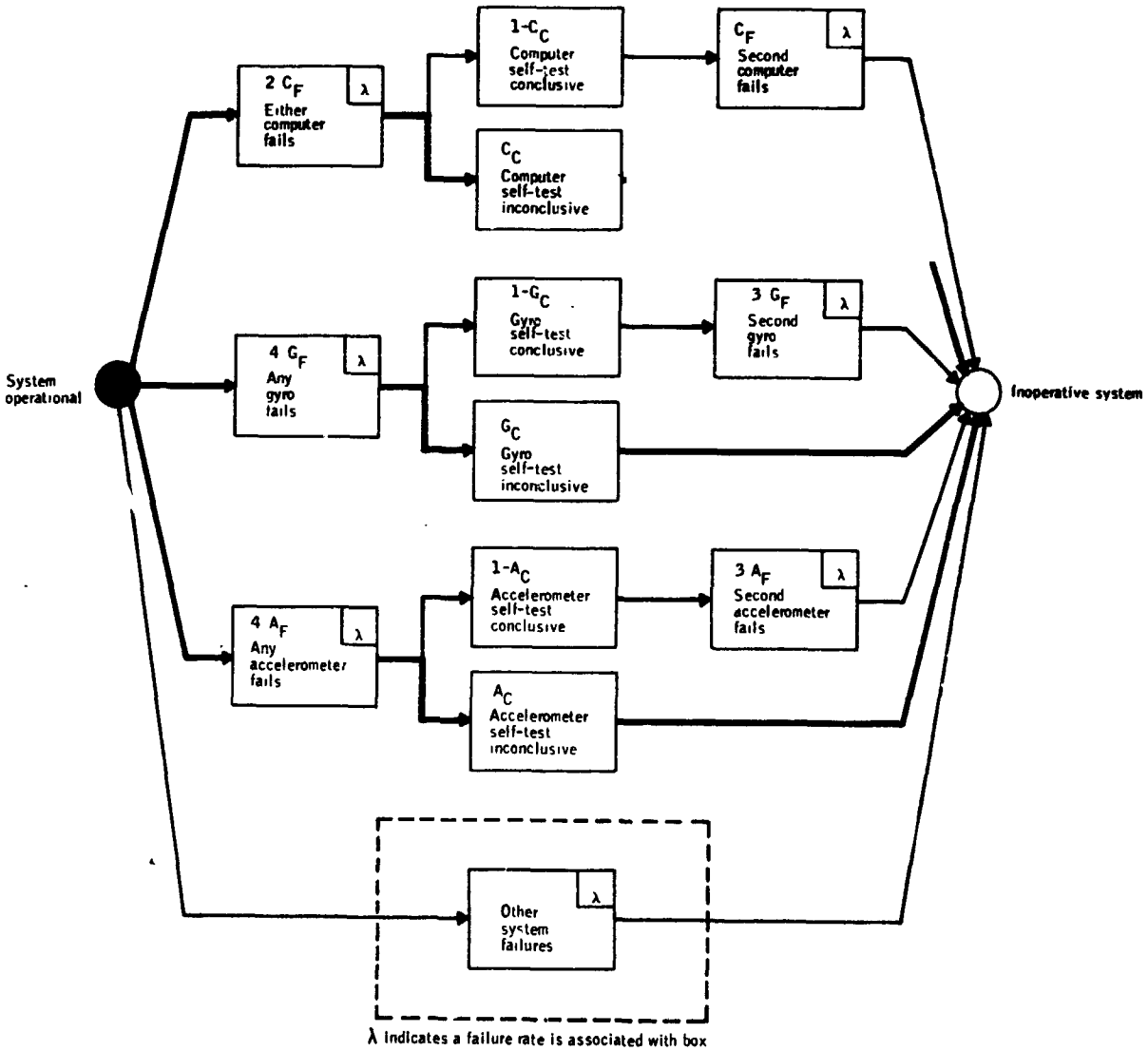


Figure 9. - Inoperative system diagram

The above equation can be simplified by eliminating all multiple identical failures (i.e., two gyros, two accelerometers, two computers) because the failure probability resulting from these paths is several orders of magnitude smaller than the dominant paths. The equation reduces to

$$P_A = (2C_F \cdot C_c + 4G_F \cdot G_c + 4A_F \cdot A_c)t$$

where

C_F = computer failure rate/hr

C_c = computer test deficiency

G_F = gyro failure rate/hr

G_c = gyro test deficiency

A_F = accelerometer failure rate/hr

A_c = accelerometer test deficiency

t = mission time in hours

Design failures versus random failures.- A distinction is made between random failures and failures which occur due to design deficiencies in the hardware or software that preclude satisfactory operation over the complete operational envelope. The latter failures may appear as simultaneous failures during actual operation and are not the type of failures given consideration in this report.

Dual-channel computers with output comparison monitoring.- Figure 10 is the failure diagram for a dual-channel computer configuration where each computer provides comparison monitoring of its outputs with the other computer by the digital intercom bus. Detection of the first computer failure approaches an effectiveness of 100%. Effectiveness of isolation of the first computer failure is determined by the computer self-test effectiveness. A sensor failure is detected by the computer by summing the sensor signals, but actual isolation of the failure is dependent on the individual sensor self-test. This diagram illustrates the system status for various failure

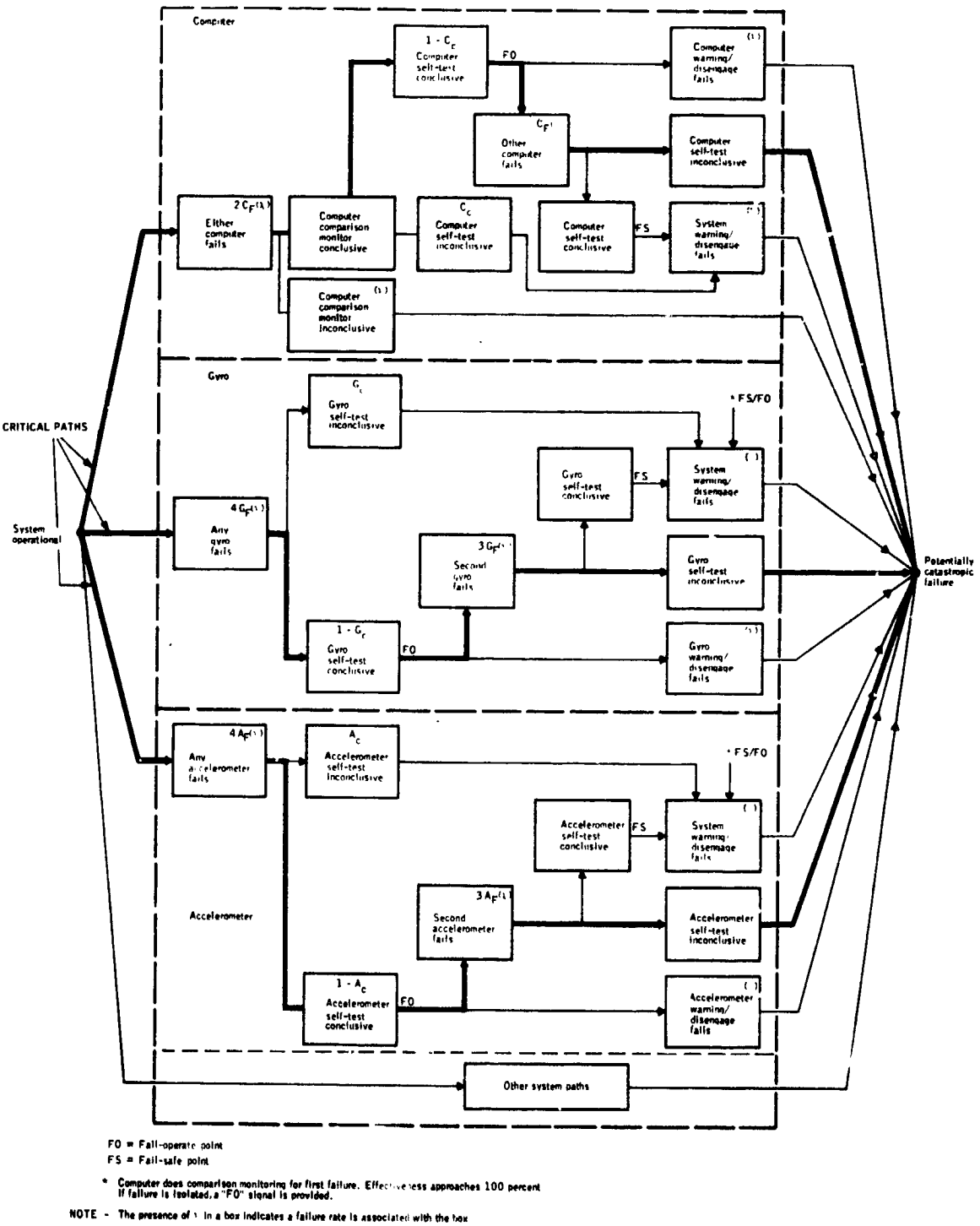


Figure 10. - Dual-channel computer with comparison monitoring failure diagram

situations, including the fail-operate condition, the fail-safe disengage conditions, and the potentially catastrophic conditions for the computer and the sensors.

A potentially catastrophic failure has occurred when the system experiences a failure but does not disengage or present a warning light in the cockpit. This point is shown on the right side of Figure 10 and may be reached by many paths originating from the point labeled "system operational." The dark lines entitled "critical paths" are the dominant failure modes for this configuration. The comparison monitoring of the computers effectively removes the possibility of not detecting the first computer failure such that the P_{CF}s for the critical path are now determined largely by the self-test capability of the computers and sensors.

The fail-operate points are shown by "FO" on Figure 10. These points may be located by following a path (left to right) which include a single failure and a self-test-conclusive box. The "FO" points mean that the failure has been detected by the computer and subsequently isolated by self-test, thus permitting the system to remain operative. A warning light is activated in the cockpit indicating a failure has occurred, but the system remains operative.

The fail-safe points are shown by an "FS" on Figure 10 and mean that a failure has been detected but not isolated. A warning light is activated in the cockpit indicating a failure has occurred and that the system can no longer be relied upon and has been automatically disengaged or should be manually disengaged. In the case of the box entitled "system warning/disengage fails," the first failure is indicated in the cockpit as "FS" if the failure cannot be isolated.

For this configuration, the P_{CF} can be approximated by considering only the indicated critical paths because the probability of a potentially catastrophic failure in the other paths is at least an order of magnitude smaller. The P_{CF} equation using Appendix D and Figure 10 reduces to:

$$P_{CF} = (C_F{}^2 C_C + 6G_F{}^2 G_C + 6A_F{}^2 A_C)t^2$$

where

C_F = computer failure rate/hr

C_C = computer test deficiency

G_F = gyro failure rate/hr

G_C = gyro test deficiency

A_F = accelerometer failure rate/hr

A_C = accelerometer test deficiency

t = mission time in hours

This formula can either be used to find the expected P_{CF} given the self-test deficiency for the sensors and computer or to find the needed self-test for any one function given all of the other numbers. Figure 11 is a plot of

$$\frac{P_{CF}}{t^2} = C_F{}^2 C_C + 6F_F{}^2 G_C + 6A_F{}^2 A_C$$

for the following set of conditions:

$C_C = G_C = A_C$ (component self-test deficiencies are the same)

$C_F = 2.1 \cdot 10^{-4}$ (failure/hour)

$G_F = 0.5 \cdot 10^{-4}$ (failure/hour)

$A_F = 0.4 \cdot 10^{-4}$ (failure/hour)

Adding the computer comparison monitoring to the first configuration practically eliminates the probability of a catastrophic failure in the computer because computer failures are readily detected. If the failure is not isolated, a fail-safe configuration results.

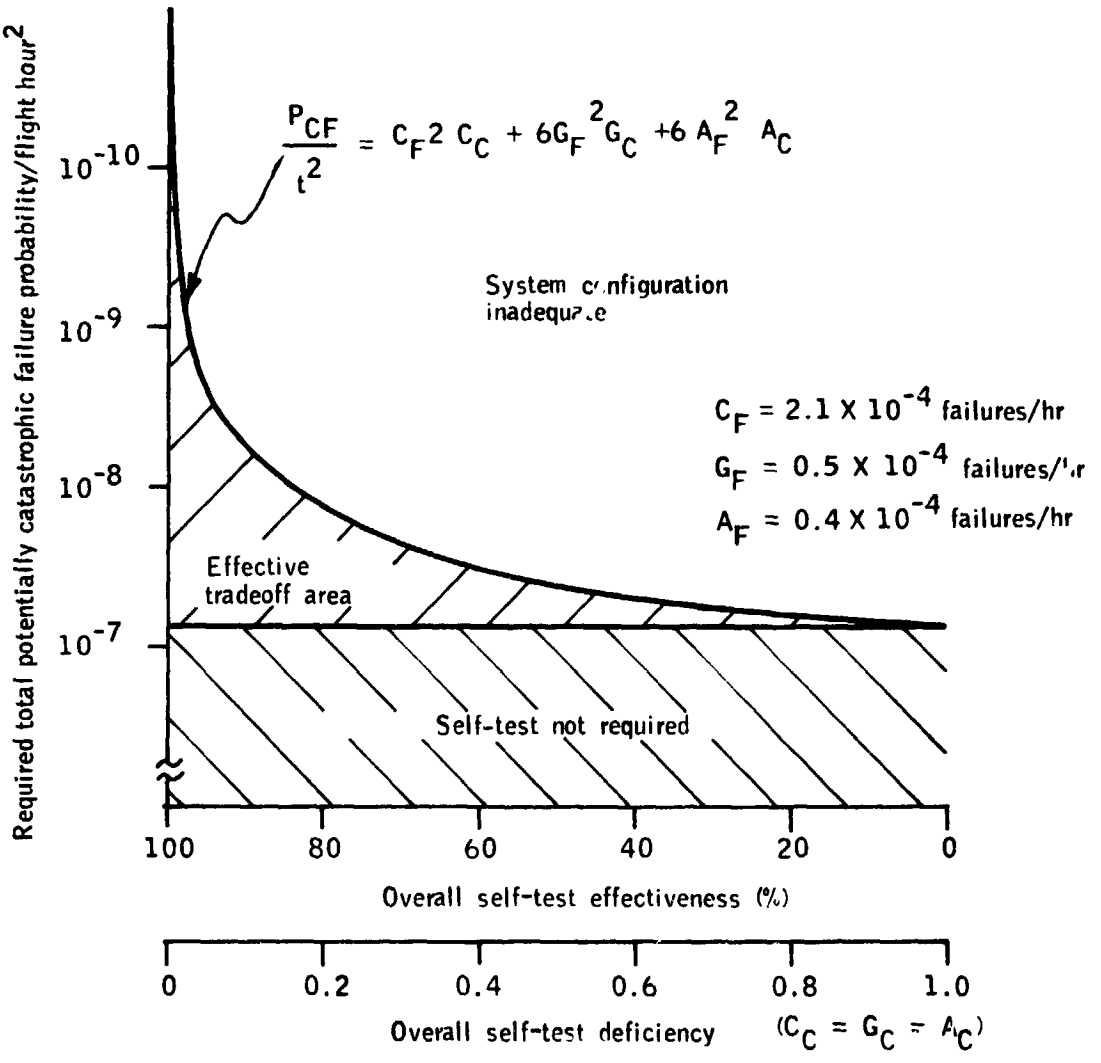


Figure 11. - Effect of self-test on flight safety for a dual-comparison computer

This condition is preferred over the first system discussed (Figure 7) because a decrease in P_{CF} (increase in safety) by three orders of magnitude is obtained by only slightly increasing overall complexity. A self-test effectiveness of 75 to 95% will provide P_{CF}/hr^2 values in the 10^{-7} to 10^{-9} range which are typical of values required to meet safety requirements. These self-test effectiveness values can be achieved without extensive failure mode and effects analysis.

The probability of an inoperative system (P_A) is the same as discussed for the dual-channel computer configuration (except for the failure rates of the computer comparison monitor circuitry which are small).

The effectiveness of dual-channel computers with and without output comparison monitoring is summarized in Table 1.

Effect of Self-Test on Fail-Operational Performance

The self-test capabilities of the sensors and computers directly determine the probability of an inoperative system (P_A). Figure 12 shows the relationship between self-test and an inoperative system and is based on the failure rates shown. This figure and Figure 9 (inoperative system diagram) apply to either the dual computer or dual computer with comparison monitoring configurations, and, as such, the fail-operational capability of both systems is the same. The fail-operational requirements may impact the self-test effectiveness as does the catastrophic failure requirement.

Self-test nomograph. - In the previous illustration a common self-test deficiency was applied to the computer and sensors. In reality a tradeoff exists between the self-test capability of each sensor set and the computers. Figure 13 shows the self-test tradeoff for the complete system and is a nomograph of the previously derived formula:

$$\frac{P_{CF}}{t^2} = C_F{}^2 C_C + 6G_F{}^2 G_C + 6A_F{}^2\, 2A_C$$

TABLE 1. - DUAL-CHANNEL TETRAD EFFECTIVENESS WITH AND WITHOUT COMPUTER COMPARATOR

Probabilities	Without computer comparator		With computer comparator	
	Equation	Value	Equation	Value
P_{CF} = probability of a potentially catastrophic failure	$P_{CF} = (2C_FC_C)t$	$3.66 \cdot 10^{-5}$ (t = 1 hr)	$P_{CF} = t^2(C_F^2C_C + 6G_F^2G_C + 6A_F^2A_C)$	$5.015 \bullet 10^{-9}$ (t = 1 hr)
P_A = probability of the system becoming inoperative	$P_A = t(2C_FC_C + 4G_FG_C + 4A_FA_C)$	$5.66 \cdot 10^{-5}$ (t = 1 hr)	$P_A = t(2C_FC_C + 4G_FG_C + 4A_FA_C)$	$5.66 \bullet 10^{-5}$ (t = 1 hr)
P_{FS} = probability of a fail-safe condition	$P_{FS} = (P_A - P_{CF})t$	$2.00 \cdot 10^{-5}$ (t = 1 hr)	$P_{FS} = (P_A - P_{CF})t$	$\simeq 5.66 \bullet 10^{-5}$ (t = 1 hr)
MTBF = mean time between failure	$MTBF = \frac{1}{2C_F + 4G_F + 4A_F}$	1282 hr	$MTBF = \frac{1}{2C_F + 4G_F + 4A_F}$	1282 hr
MTBLF = mean time between loss of function	$MTBLF = \frac{1}{2C_FC_C + 4G_FG_C + 4A_FA_C}$	17,668 hr	$MTBLF = \frac{1}{2C_FC_C + 4G_FG_C + 4A_FA_C}$	17,668 hr

One-hour values were calculated using the following:

$C_F = 2.1 \times 10^{-4}$ failures/hr $\quad C_C = .08$

$G_F = 0.5 \times 10^{-4}$ failures/hr $\quad G_C = .035$

$A_F = 0.4 \times 10^{-4}$ failures/hr $\quad A_C = .1$ (estimated)

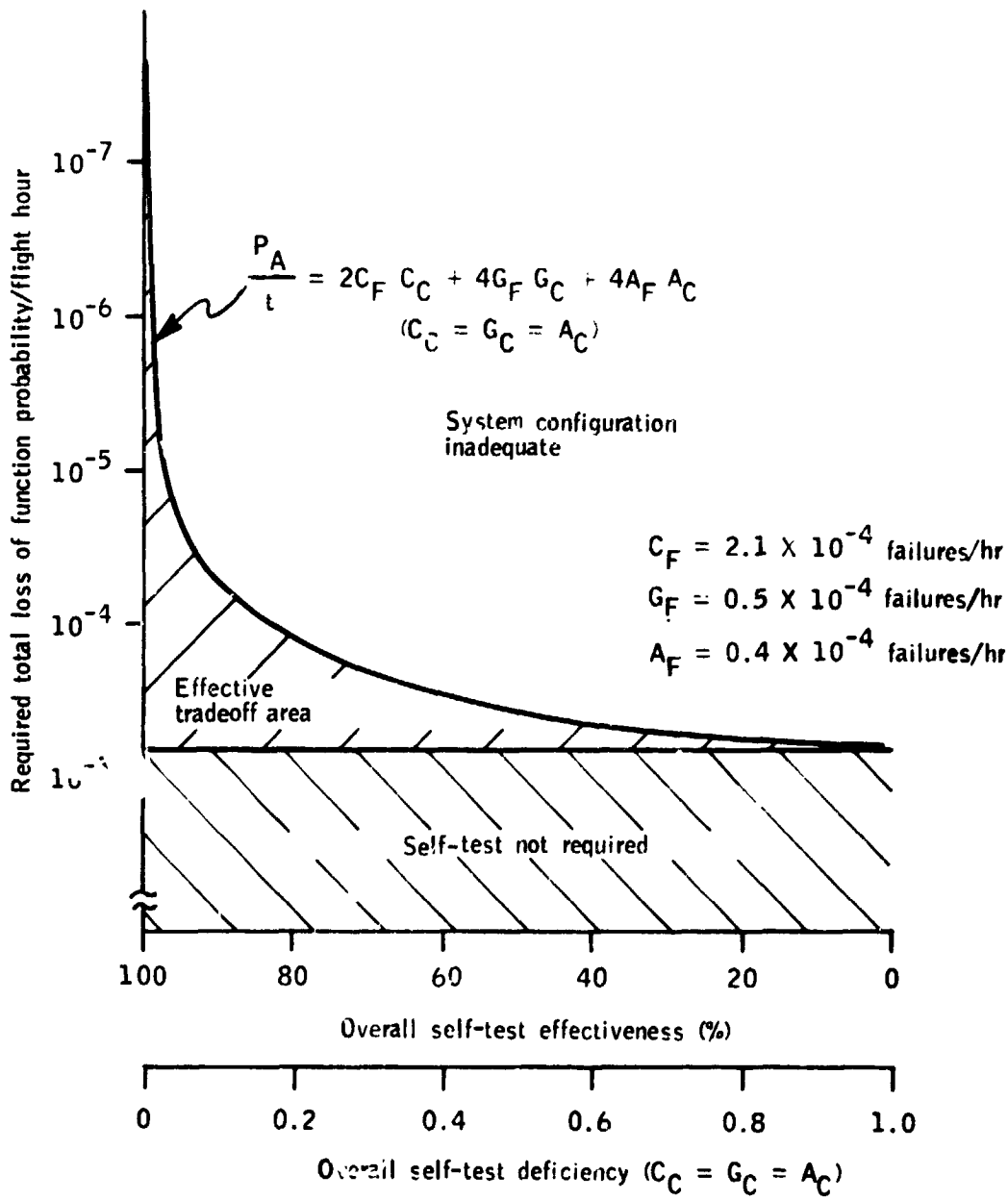


Figure 12. - Effect of self-test on fail-operational performance

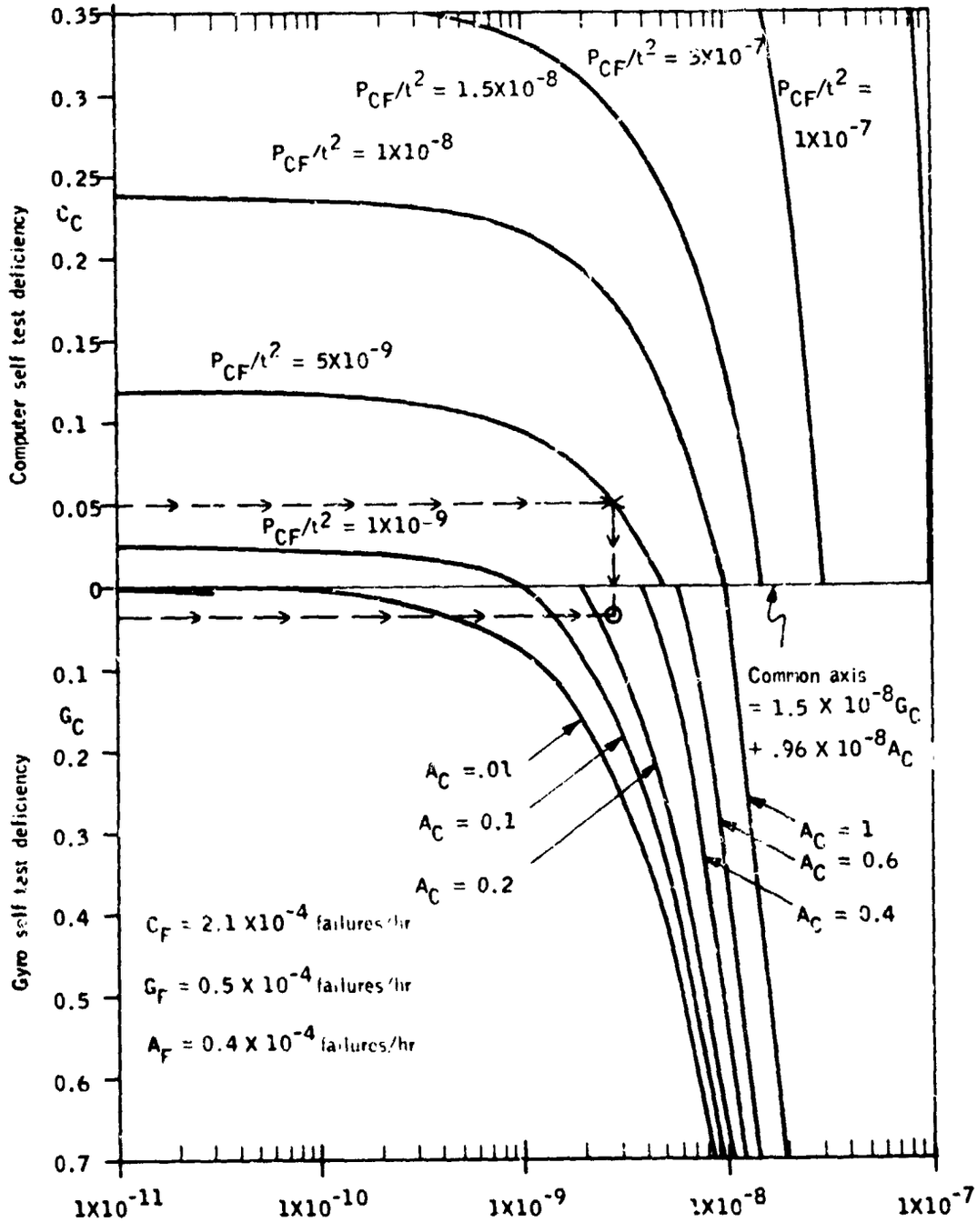


Figure 13. - Self-test tradeoff nomograph for dual computers with comparison monitoring

This chart can either be used to find the expected P_{CF}, given the self-test deficiency for the sensors and computer, or to find the needed self-test for any one function, given all other numbers. To find the expected P_{CF} draw horizontal lines corresponding to the computer and gyro self-test deficiencies. Then, draw a vertical line from the intersection of the gyro deficiency and the accelerometer deficiency curve. The point the vertical line intersects the computer deficiency horizontal line is the expected P_{CF}/t^2. The value shown on this curve is then multiplied by the square of the mission time to get the expected probability of a potentially catastrophic failure.

An example of using tradeoff figure to get an accelerometer self-test requirement would be: Given mission time of 5 hours ($t^2 = 25$) and given $P_{CF} = 1.25 \times 10^{-7}$/flight, $P_{CF}/t^2 = 5 \times 10^{-9}$. Assuming computer self-test deficiency = .05 and gyro self test deficiency = .035, you need accelerometer self-test effectiveness = 75% (.25 self test deficiency).

SECTION 4
LASER GYRO FAILURE DETECTION AND ISOLATION

The laser gyro, a recent development in optical technology, combines the properties of the optical oscillator, the laser, and general relativity to produce an integrating rate gyroscope. Remarkable features of the laser gyro include the absence of a spinning mass, simplicity of construction, inherent digital output, and capability of wide dynamic range with high resolution and accuracy.

The laser gyro concept is based on the principle that the distance around a closed optical path in a rotating frame of reference depends on the direction the path is traversed. For example, a beam of light traveling around a path in the direction of rotation will have to travel further than one traveling against the direction of rotation. This difference in path length is proportional to the rate of rotation and can be used to measure angular motion. In general, these path-length differences are exceedingly small and could not be measured before the advent of the laser. For example, a triangular laser gyro having a 50-cm path, rotating at 10 deg/hr would produce a path length difference of 10^{-4} Angstroms.

The ring laser converts this path-length difference into a measurable frequency difference because the frequency of laser oscillation depends directly on the distance around the resonator. A 50-cm ring laser oscillating at 5×10^{14} Hz would give a measurable 10-Hz frequency difference for an input of 10 deg/hr. The light leaking through one of the laser mirrors is used for obtaining the rotation information. The counter-traveling laser beams are combined by a simple optical system into an interference fringe pattern. The motion of this fringe pattern gives information on both magnitude and direction of rotation.

Honeywell has emphasized laser gyro design factors that minimize any disturbance in the measurement of these small path differences. This has led to the use of ultra-low-expansion CerVit glass ceramic to form the stable ring laser structure that establishes the basic path length. This material has a very low temperature coefficient of expansion and is compatible with the hard-vacuum technology required to generate the laser light source. CerVit is also characterized by low helium diffusion which is required for a long-life, stable laser.

There is a lock-in phenomenon associated with the two counter-traveling laser beams. When the frequency difference between the two oscillators becomes low, on the order of 1000 Hz, the two oscillators are "pulled" in frequency towards each other. This pulling is caused by coupling which occurs at the mirrors and is a function of backscattering of light. An oscillating mechanical dither technique is used to substantially reduce the amount of time the gyro is in the lock-in region, thereby reducing the lock-in error.

The GG1300 laser gyro is shown in Figure 14. The required electronics are mounted inside of the gyro case where they are protected from the environments. The CerVit block is shown attached to the center post by clamping springs used for oscillating mechanical dither lock-in compensation.

The laser gyro has been divided into six functional areas for a reliability analysis. These areas are shown in the functional block diagram of Figure 15 and are:

- Readout assembly
- Block assembly
- Current control
- Case assembly
- Dither assembly
- Path length

Figure 14. - GG1300 laser gyro

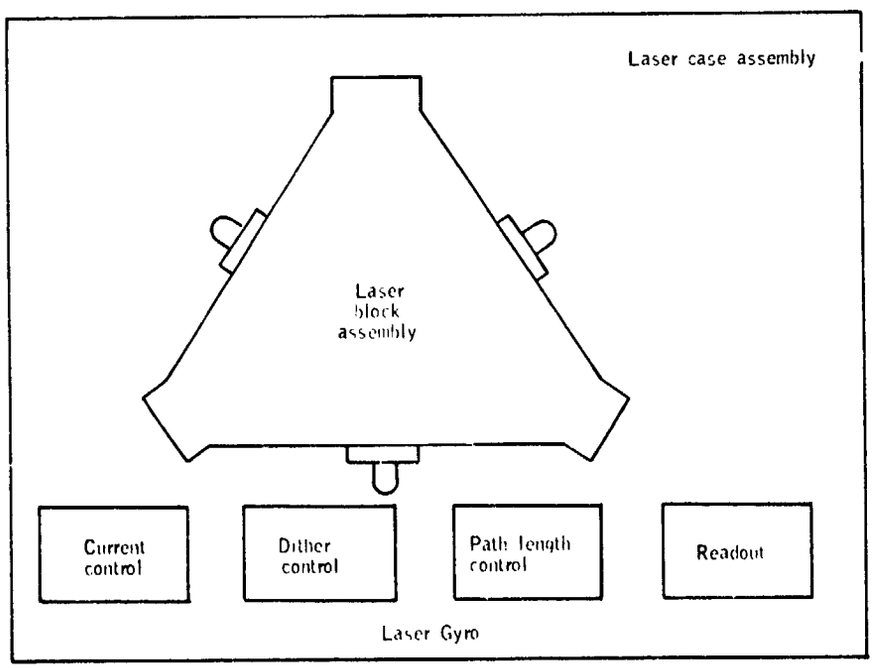


Figure 15. - Laser gyro reliability functional block diagram

Readout Control Circuitry

Description. - The laser gyro has two laser beams, one propagating clockwise around the cavity and the other propagating counter-clockwise. The two beams are optically combined outside the cavity into a fringe pattern. The motion of the fringe pattern is detected by a dual-photodetector, amplified and converted into a pulse rate. A logic circuit separates the gyro output pulses into two groups: one group proportional to clockwise rotation of the laser gyro, and the other proportional to counter-clockwise pulses. This raw output is then buffered by line drivers. The block diagram of the readout circuitry is shown in Figure 16.

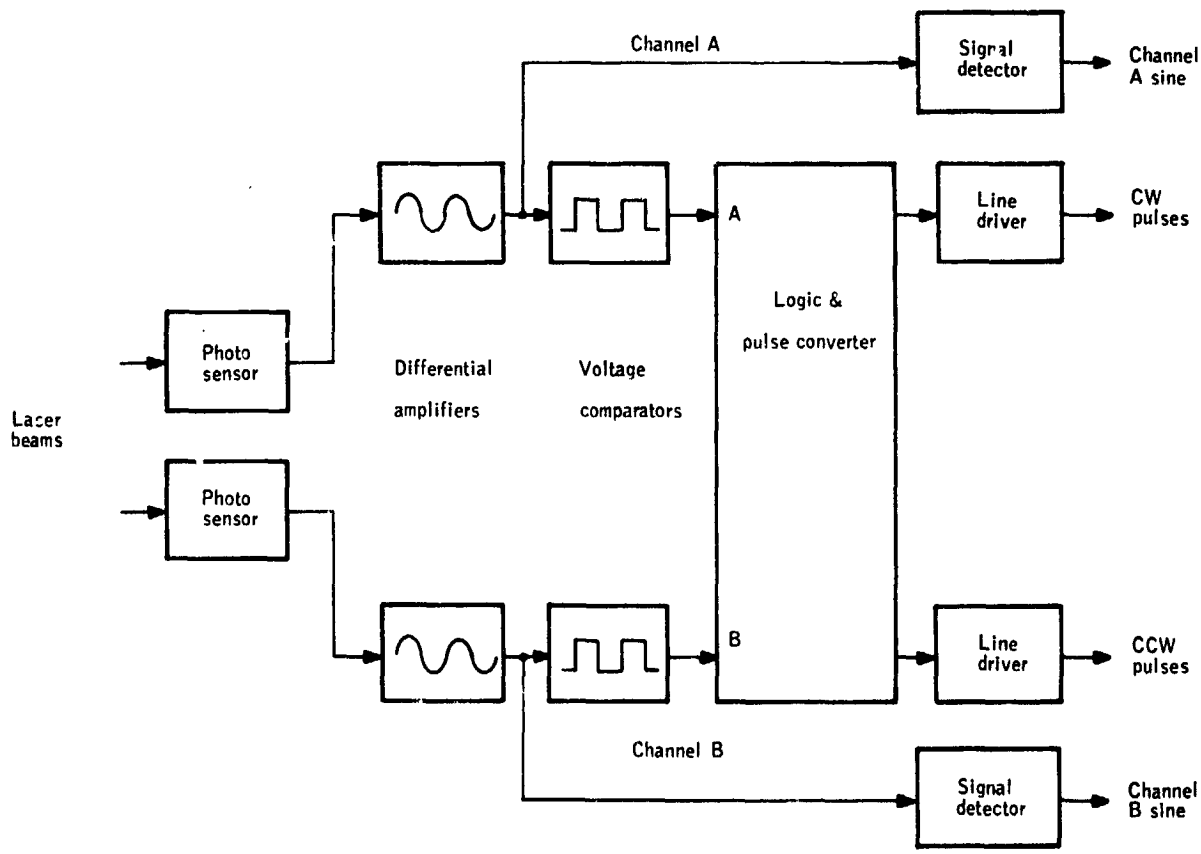


Figure 16. - Gyro readout circuit

Analysis of the readout circuit reveals the following:

- The sum of the gyro CW and CCW counts is equal to or less than the counts measured at either of the photosensor channel outputs which feed the logic (points A and B on the logic block).
- The counts measured at A may or may not equal the counts measured at B.

The function of the logic and pulse converter is best understood by use of a four-quadrant state diagram (Figure 17).

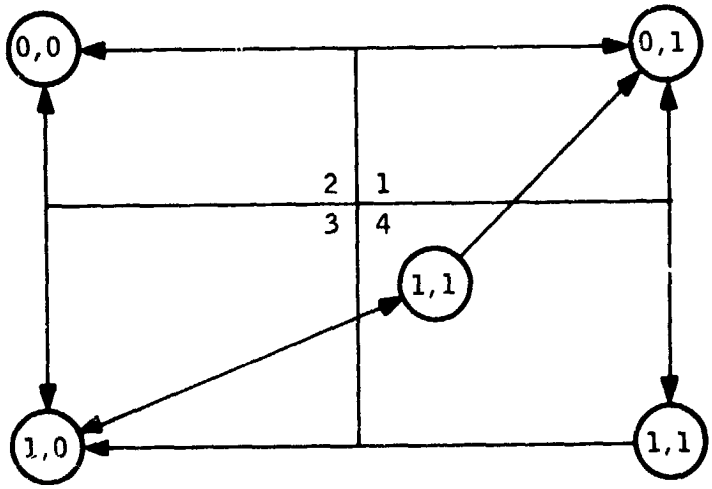
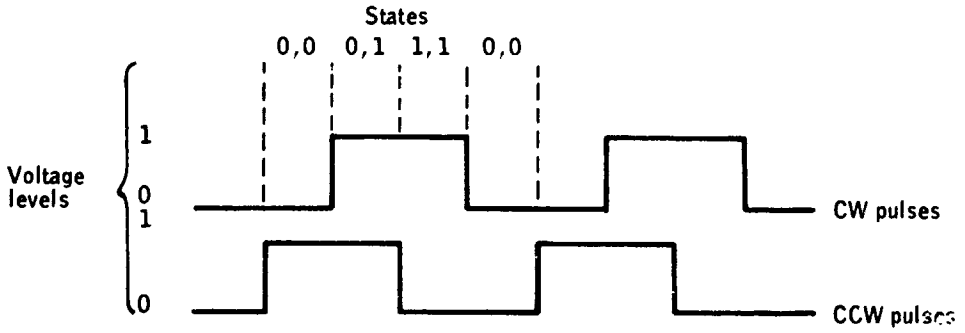


Figure 17. - State diagram

A CW pulse is generated any time the (0, 1) (1, 1) and (1, 0) states occur sequentially. A CCW pulse is generated any time the (1, 0) (1, 1) and (0, 1) states occur sequentially. This latching arrangement reduces the generation of unnecessary CW and CCW counts due to small oscillations about the input axis. The states refer to the signal levels coming to the logic and pulse converter (Figure 16) and are generated in accordance with the following diagram.



Reliability. - Table 2 summarizes the work done in each functional area to determine its applicable failure rate. This failure rate is determined by summing the individual component failure rates. Failure rates are generally expressed in percent per 1000 hours where 100% per 1000 hours equals one failure per 1000 hours.

Table 2 shows the elements included in the determination of the failure rate (.598 %/1000 hrs) for the readout circuitry or twice that for a redundant readout circuit (1.196 %/1000 hrs).

Failure Detection. - The gyro output (clockwise pulses and counter-clockwise pulses) may be partially validated by external checks performed by the computer. The output is a function of input rate and without knowledge of the input rate the output cannot be checked for accuracy as it may vary up to plus or minus several hundred thousand pulses per second. However, there is a phenomenon around zero input rate caused by dither spillover which is a function of the misalignment between the mechanically dithered quartz block and the pickoff. The physical motion produced by the mechanical dither motion is a few thousandths of an inch and is not apparent to a human observer. This dither angle must be removed from the readout as it can produce uncertainties in the output angle, limit the time between accurate measurements, or cause computer errors to be introduced.

The dither angle is removed from the gyro output by design of the gyro readout optics which removes this dither angle, instant by instant, from the gyro output.

TABLE 2. - COMPONENT FAILURE ANALYSIS

Component	λ	Functional blocks											
		Case		Block		Readout		Dither		Path length		Current control	
		n	nλ	n	nλ	n	nλ	n	nλ	n	nλ	n	nλ
Capacitor													
• Ceramic	.0015					27	0405	12	018	10	.015	11	.0165
• Solitant	0045					1	0045	2	009	5	022	2	.009
• HS plastic	.01									2	020		
Diodes													
• CP silicon	0045							2	009	1	.0045	2	.009
• Zener	.008					1	008			7	056	3	.024
• CP (com)	014							1	014			2	.028
• Zener (com)	024											2	.028
Microcircuit													
• Analog	.05					4	.2000	4	2000	4	2000	2	1000
• Digital	005					4	0200						
• CMOS	05									2	1000		
Resistor													
• RC	.0005					32	0160	21	0105	10	.0200	10	005
• RN	0025					14	035	5	0125	2	.005	12	.030
• RW (com)	015									2	030	2	.030
Transistor													
• FET	.015											2	030
• Dual	039					2	078						
• CP	0065							2	.013	4	.026	2	.013
Piezo actuator	.001							32	.032	2	002		
Readout sensor, dual	.18					1	.18						
Path-length sensor	.09									1	09		
Connections	$001\sqrt{N}$	31	0056	3	.0017	254	016	133	.012	200	.014	133	.012
Connector	01	2	0200										
Cervet block and mirrors	452			1	452								
Cathode life					2.000								
Case seal		1	05										
Total λ (%/1000 hrs)			0756		2.4537		.5980		3300		6045		.3345

λ failure rate in percent per 1000 hours where one failure equals 100% per 1000 hours.

† 196 for redundant readout

Laser Block Assembly

Description. - The structure and function of the Honeywell GG1300 laser gyro block assembly is set forth in the following paragraphs.

The two main elements of the ring laser are the resonator and the amplifier. In the solid-block design, the resonator contains only two elements, the mirrors and the aperture. The ring laser cavity is generated by a set of three mirrors placed to form a closed optical path that is an equilateral triangle. All three mirrors have the same reflectivity. In this approach the ring laser geometry is precisely defined by the solid block.

The gyro readout is shown in Figure 16. The readout corner cube is placed so that the CW beam is superimposed on the CCW beam at an angle controlled by the wedge angle of the readout mirror. This creates the fringe pattern shown and permits up-down counting of the output phase difference of the two oscillators.

The readout corner cube prism which translates and returns the laser output is fixed to the gyro base. The gyro readout mirror therefore moves with respect to this prism. The path length in the readout system is increased and decreased as the two elements move with respect to each other. By dithering the gyro about a point slightly removed from the center of the gyro, this path difference in the readout is made equal and opposite to the fringe motion created by the gyro oscillator phase changes. The cancellation is instant by instant, with the readout detectors thus "seeing" a fringe motion equal to the base motion of the gyro with a small residual dither amplitude. The residual dither motion (uncompensated dither) is defined as dither spillover.

Figure 18 is an input/output curve which illustrates the effect of dither spillover on pulse count. Dither spillover is normally adjusted to be below ±1.0 count per cycle. For this scheme it would be adjusted between .5 counts/cycle and 1.0 counts/cycle. For a positive input rate near zero, the CW pulses do not vary as a function of input rate, but remain constant while the actual input rate is determined by subtracting the CCW pulses from the CW pulses for a given time period $[\Sigma (P_{CW} - P_{CCW})]$. The same is true for the CCW pulses and a negative input rate. This phenomenon is very useful in detecting failures, inasmuch as zero pulses during a given time period does not mean zero rate but a failure (Figure 19).

Appendix C contains descriptions of various readout configurations of which two provide redundant readout circuitry. For these configurations, the computer can compare the multiple readouts to ensure the circuitry is working correctly.

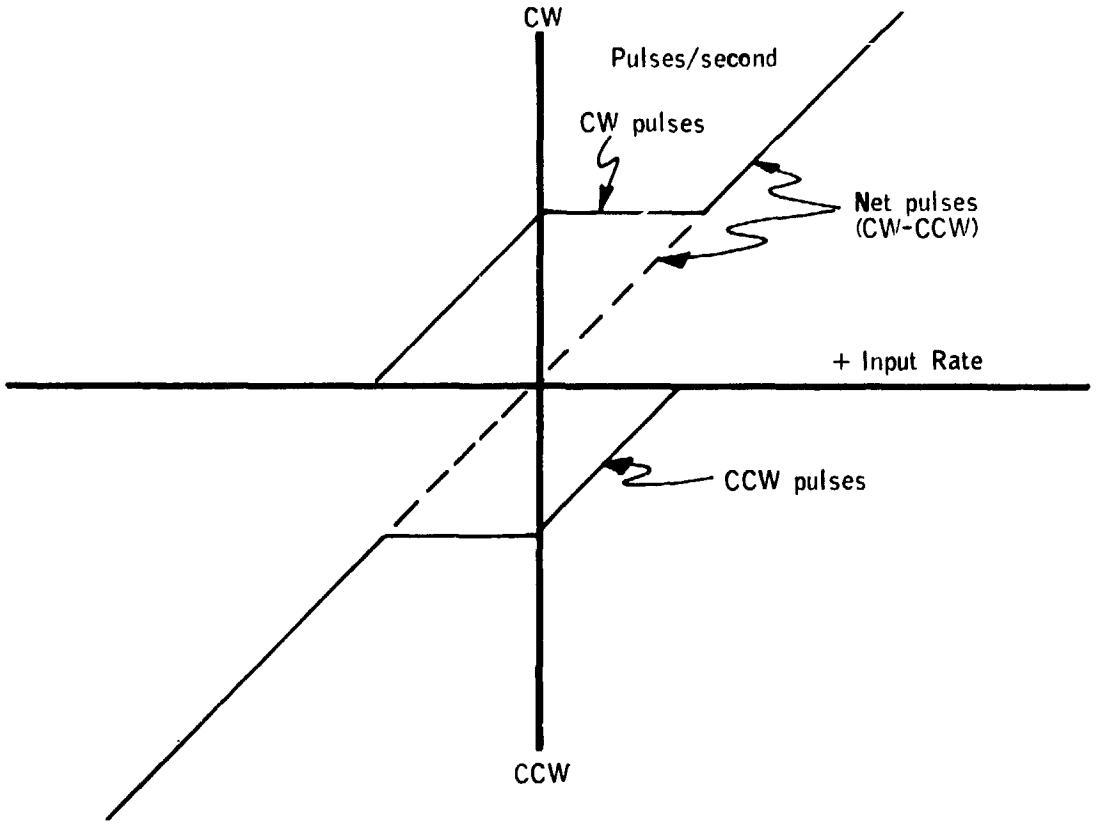


Figure 18. - Input/output curve (± count spillover)

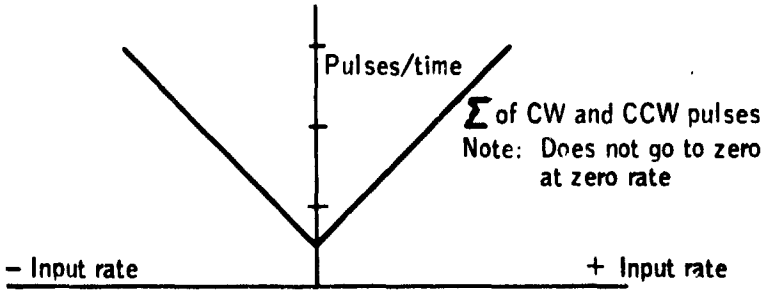


Figure 19. - Pulses/time versus input rate

Appropriately drilled holes permit passage of the oppositely-directed traveling waves. These holes serve as apertures and, when filled with a low pressure of helium and neon, as gain tubes. A single large cathode and two anodes establish the split balanced d-c discharge. This permits precision gain control and trimming of null offsets.

The optical path length is precisely controlled to an integral multiple of the lasing wavelength by a piezoelectrically driven transducer mirror. Control is maintained to the peak laser power for optimum performance and temperature capability.

The light leakage through the multilayer dielectric flat mirror is used for obtaining the rotation signal. The two beams are folded together by a simple optical system to form an interference pattern on a dual photosensor. The cube corner is mounted to the base, producing a signal that exactly counteracts the gyro-created dither signal. The net readout is therefore the true rotation of the gyro in inertial space.

Gyro dither is obtained from a very simple piezoelectric motor. PZT elements are bonded onto both sides of the reeds of the dither spring which supports the block. Acting push-pull, the PZT elements create bending moments in the reeds and create an oscillating input (dither) to the ring laser.

Reliability. -- Table 2 shows the elements included in the determination of the failure rate (2.454 %/1000 hrs) for the block assembly. This includes a 2% failure rate per 1000 hours for the cathode life. The wearout mechanism that limits lifetime in the laser gyro is the gas pumping action of the cathode. To sustain the laser gas discharge, positive ions collide to provide electron emission. Some ions are trapped during this process, and other gas atoms are buried by the sputtered cathode material. Thus, when the discharge is run, a small amount of helium and neon is pumped by the cathode. Over a period of time this results in reduced gas pressure and eventual gyro failure. Based on accelerated life-test results, estimates for the wearout life due to cathode pumping is 50,000 hours. *

Based on accelerated life-test results, estimates for the wearout life due to cathode pumping is 50,000 hours.*

An approximate equivalent MTBF for gyros having both a random and wearout (normal) failure distribution can be computed using the following equation:

$$(MTBF)_{equivalent} = \frac{1}{\lambda}(1-e^{-\lambda T})$$

where

λ = random failure rate
T = mean in hours of wearout distribution

Using 2.99% per 1000 hours (random) from Table 2 and 50,000 hours (mean life) for the laser gyro yields an MTBF of 25,900 hours. A 20,000 hour MTBF is indicated by Table 2 if no distinction is made between random and wearout failures. The more conservative of the two estimates is used in the report.

Failure detection. - The integrity of the laser block assembly can best be monitored by analyzing the channel A sine and channel B sine signals (Figure 16). The presence of a sinewave signal on both channels indicates that an interference pattern is being generated internally in the block and is being sensed by the photosensors. The contrast or amplitude of the signal will decrease if the gas in the block becomes contaminated or there is a leak. A faulty pickoff, in terms of an alignment shift or mirror deterioration, would also reduce the amount of signal. When the amplitude of the signal drops below a predetermined level, a failure is imminent.

*Wearout life due to cathode pumping was reported as 30,000 hours in CR-137585 ("Strapdown Cost Trend Study and Forecast"). This figure has now been revised to 50,000 hours based on ongoing tests.

The present channel A sine and channel B sine signals are brought out with an RC circuit which is valid for monitoring to about 10 kHz, beyond which the output drops off. Isolation amplifiers and level detectors would be substituted for the RC networks to prevent high-frequency rolloff to provide fault detection over the complete operating range.

Current Control Circuitry

Description. - The laser gyro discharge is initiated by applying a high-voltage d-c potential between the anode and cathode. This voltage, typically twice the operating potential required to sustain the discharge, is sufficient to cause ionization discharge within several milliseconds after the circuit is energized. After discharge is initiated, it is immediately regulated by the current control circuits.

Discharge current control is required to stabilize gain and to balance the two discharge current paths. Variations in total current cause gain changes and result in a small scale-factor variation; variation in the current balance results in a null shift in the gyro output.

Figure 20 shows the design of the discharge current control. Laser gyro configurations have one cathode and two anodes so that there are two distinct current paths in the gyro discharge.

Differential discharge current control is accomplished by a FET control element in each current path. The total current ($I_1 + I_2$) flows through the bridge which measures the differential current ($I_1 - I_2$). The current unbalance ($I_1 - I_2$) is sensed by a differential amplifier. The output signal of the amplifier drives the FET transistors, maintaining a given current balance in the presence of disturbances.

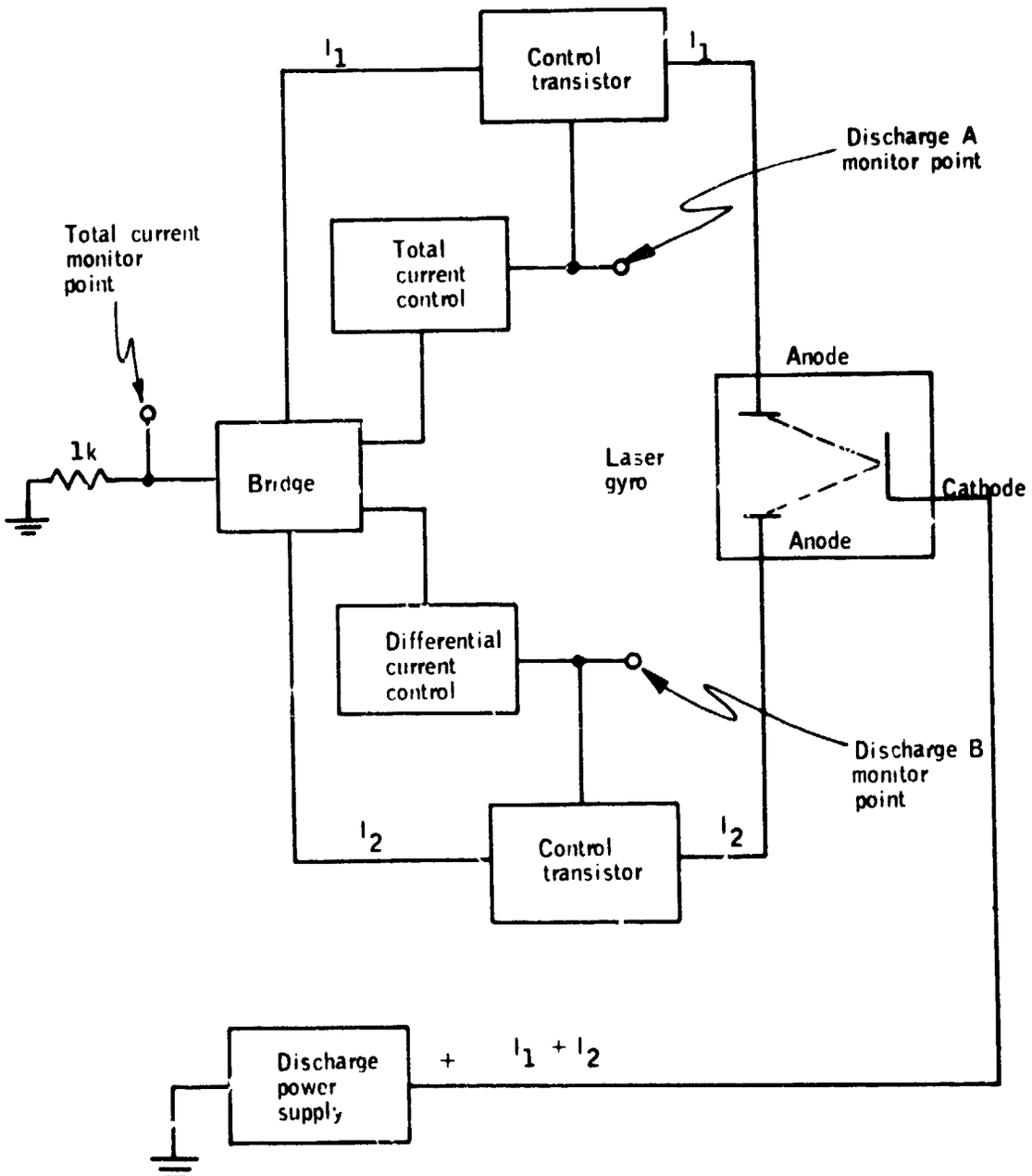


Figure 20. - Discharge control circuit

Reliability. - Table 2 shows the elements included in the determination of the failure rate (.3345 %/1000 hours) for the current control circuitry.

Failure detection. - Total current (discharge current) is monitored to determine that the operating point of the laser gyro has not shifted. A shift in operating point is indicative of a change in the gyro bias. Currents I_1 and I_2 are monitored to make sure the control loops are working and not driven into saturation.

Case Assembly

Description. - The case assembly is sealed to protect the laser block and electronics from environmental contaminates (dirt, salt, moisture, etc.) and to provide an internal gas pressure which does not vary with altitude, thus minimizing high-voltage arcing problems.

The center post of the case assembly must support and maintain the alignment of the laser block relative to the case mounting surfaces.

Reliability. - Table 2 shows the elements included in the determination of the failure rate (.0756 %/1000 hr) for the case assembly.

Failure detection. - The most probable failure modes of the case involve failures associated with the case seal and the connector. These failures subsequently produce failures in the gyro electronics, and a case seal failure or a connector failure is detected when the electronics failure is signaled. The high-voltage circuitry is the most sensitive to its environment, and a case seal failure would probably affect this circuitry first. The self-test capability of the case is equated to the self-test capability of the high-voltage current control circuitry. Table 3 shows the monitors relative to the gyro parameters. A case seal failure would eventually manifest itself in a failure of I_t, I_1, or I_2 which are monitored.

TABLE 3. - MONITORS VERSUS PARAMETERS MONITORED

Monitor	Gyro parameter monitored
Laser block assembly monitor	
Channel A sine	Presence of laser fringe pattern
Channel B sine	Contrast of laser fringe pattern Determines pickoff integrity
Readout assembly monitor	
External gyro output	Checks readout circuitry
Analysis	Determines presence of dither spillover (rates 360°/hr)
Dither monitor	Determines that dither loop is working
Path-length monitor	Determines laser path is an integral number of λ's (beat frequency)
Laser case assembly and current control monitor	I_T value confirms proper lasing operating point
	I_1, I_2 values confirm that current control loop is working satisfactorily

Path-Length Control Circuitry

Description. - Length control of the laser cavity is necessary in inertial-grade gyros principally because of thermal effects that cause the laser cavity to change length when wide thermal environments are encountered. Also, the initial set point must be controlled. Uncontrolled changes in length cause changes in scale factor and null, reducing the ultimate accuracy.

Length control is accomplished by a control circuit operating on the intensity of the laser beam. The variation of the laser output intensity with cavity length is characterized by a maximum near doppler center and a decrease in intensity on either side (see Figure 21). This pattern repeats as modes are scanned (frequency tuned) by a variation of cavity length.

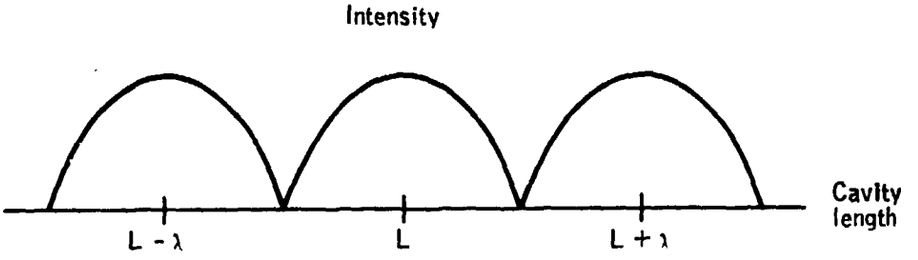


Figure 21. - Single-beam intensity versus cavity length

Stabilization of cavity length requires generation of a length reference point and a measure of the deviation from this point. The maximum of the laser intensity curve is used as a length control reference.

Deviations from this maximum are measured by a small modulation or dither of cavity length. The small modulation of length produces a small-intensity modulation which bears a fixed-phase relationship with respect to the applied dither signal. In addition, this phase relationship changes by

180 degrees in going from one side of the intensity maximum to the other. As a consequence, a discriminant is generated for use in closed-loop control to stabilize the cavity length.

Figure 22 illustrates the design of the length control.

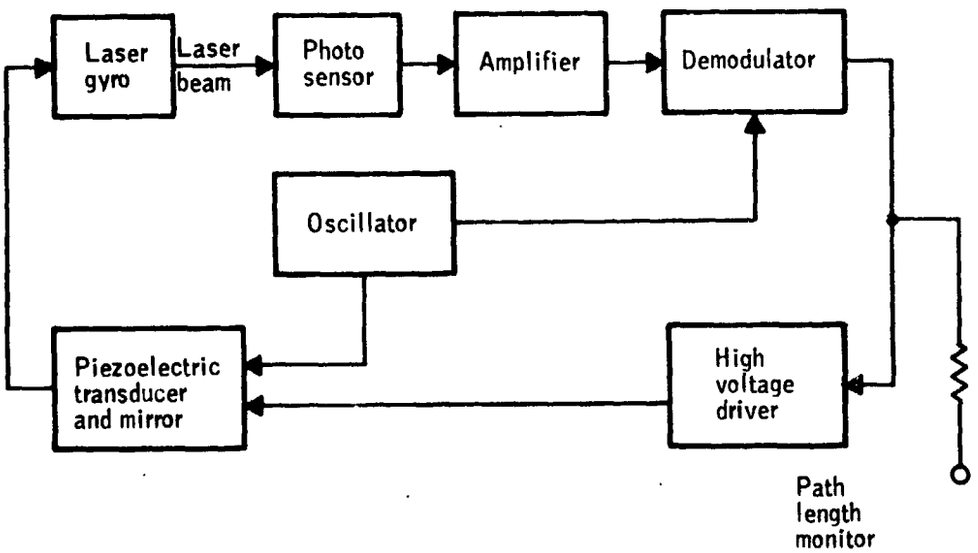


Figure 22. - Length control

The cavity length is controlled by a piezoelectric transducer which displaces one of the laser gyro mirrors. The length dither has an amplitude equal to a small percent of the mode spacing. It is generated by the oscillator and applied to the mirror through the piezoelectric transducer. The amplified photosensor signal, derived from the variation in intensity of the laser beam, is applied to a phase-sensitive demodulator which receives its reference input from the oscillator. The resulting d-c signal is proportional to the deviation from intensity maximum and has a polarity which depends on which side of the maximum the operating point is located. This d-c signal is used as an input for a high-voltage driver which applies dc to the piezoelectric

transducer. In closed-loop operation, the length control operates as a null-seeking system to stabilize cavity length at the intensity maximum. In the presence of cavity length disturbances, the d-c voltage applied to the piezoelectric transducer changes to keep the cavity length constant.

Reliability. - Table 2 shows the elements included in the determination of the failure rate (. 6045 %/1000 hours) for the path length control.

Failure detection. - Figure 22 shows the monitor for the path length control. The path length servo loop is considered to be working if the path length monitor voltage does not go above 5 volts (10 volts is saturation). A level detector is adequate for this monitor.

Dither Control Circuitry

Description. - To improve the performance of the laser gyro, a mechanical rotational bias is introduced so that the gyro operates outside the lock-in region. The bias technique consists of physically oscillating (dithering) the laser gyro about its input axis. The amplitude of this oscillation or dither is typically 200 to 400 arcseconds. The frequency is approximately 200 to 400 Hz.

The operation of the bias system is shown in Figures 23 and 24. The laser gyro, constructed as a solid quartz block, is suspended from the case by a set of cruciform springs.

A d-c torquer is attached to the suspension mechanism and the case, and provides the driving force for generating the sinusoidal bias. The inertia of the quartz block, together with the spring constant of the suspension, constitutes a mechanically resonant system.

The dither drive electronics have the function of dithering the gyro and controlling the average amplitude of this drive.

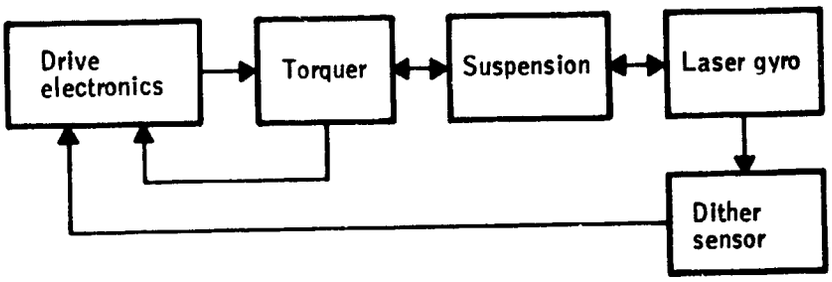


Figure 23. - Dither drive

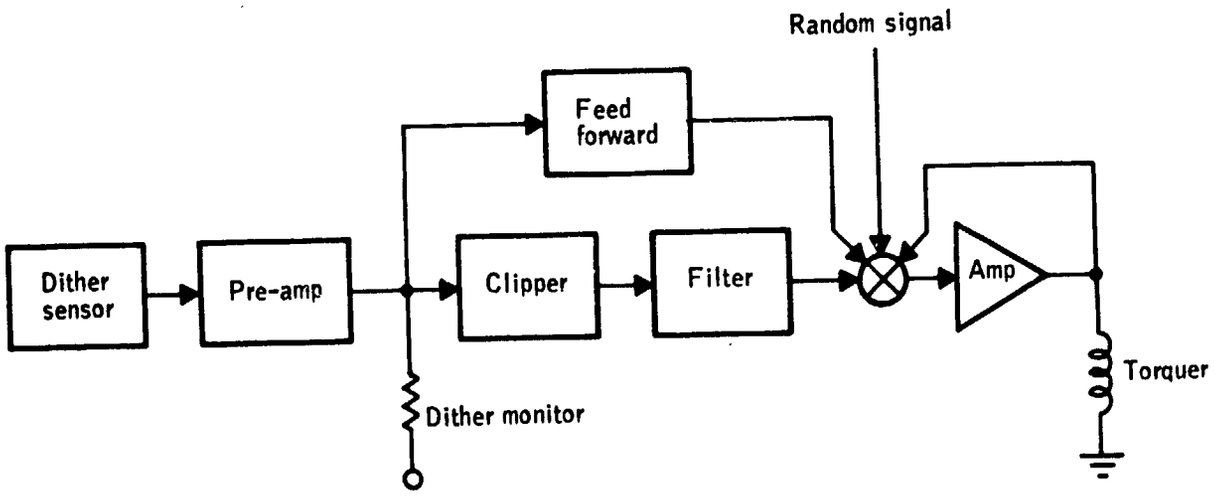


Figure 24. - Dither electronics

Reliability. - Table 2 shows the elements included in the determination of the failure rate (.33 %/1000 hr) for the dither control circuitry.

Failure detection. - Figure 24 shows the placement of the dither monitor which senses the presence of the a-c dither signal. The circuit is not working if the signal goes to zero or to a steady-state d-c level.

Gyro Failure Detection

The laser gyro design (supplemented with a redundant readout) lends itself quite readily to built-in-testing monitors. Table 3 summairzed the monitors along with the specific gyro parameters that are monitored. These parameters and monitors have been discussed previously.

Table 4 summarizes the self-test capability of the gyro (in this instance, self-test also includes a computer test of the redundant readout). The monitor description, calculated failure rate, and estimated effectiveness are shown for each of the gyro elements. The gyro test effectiveness are estimates based on similar self-monitoring techniques and circuitry from 7X7 and JA 37 digital autopilot programs. The specific self-test effectiveness numbers must be determined from a FMEA on the specific mechanization. (Typically a monitor has a single thread failure mode which precludes 100% effectiveness.)

Monitor effectiveness is approximately 95% for monitors which are activated when a given signal deviates from a nominal by a specified percentage. Examples are the monitors which monitor the laser block assembly, laser case assembly and the current control. Monitor effectiveness is increased to approximately 99% where a signal is driven to a maximum because a control loop is no longer controlling.

If the readout assembly is a redundant function, it can be checked externally by the computer. The effectiveness of this check approaches 100%.

TABLE 4. - GYRO SELF-TEST SUMMARY

Gyro element	Monitor description	Estimated monitor effectiveness, %	Calculated failure rate, %/1000 hrs
Laser block assembly	Sine wave amplitude detector	95.0	2.454
Redundant readout assembly	Computer test	99.9	1.196
Laser case assembly	Current control monitors case integrity	95.0	.076
Current control	Voltage level detector	95.0	.335
Path-length control	d-c max amplitude detector	99.0	.605
Dither control	a-c max amplitude detector	99.0	.330

Figure 25 shows the gyro failure model diagram. The validity monitors shown must be designed so that the probability of their failing is very much less than the probability of the self-test being inconclusive.

The laser gyro technology is new, and, as such, there is an incomplete knowledge of all the possible failure modes. Undoubtedly variations in the design of the monitors will be required as further work is accomplished and as more information becomes available.

The undetected gyro failure rate is the sum of the individual gyro assembly failure rates times their respective monitors' self-test inconclusive factor. In this manner, the total effectiveness of the gyro self-test is calculated at 96.5%.

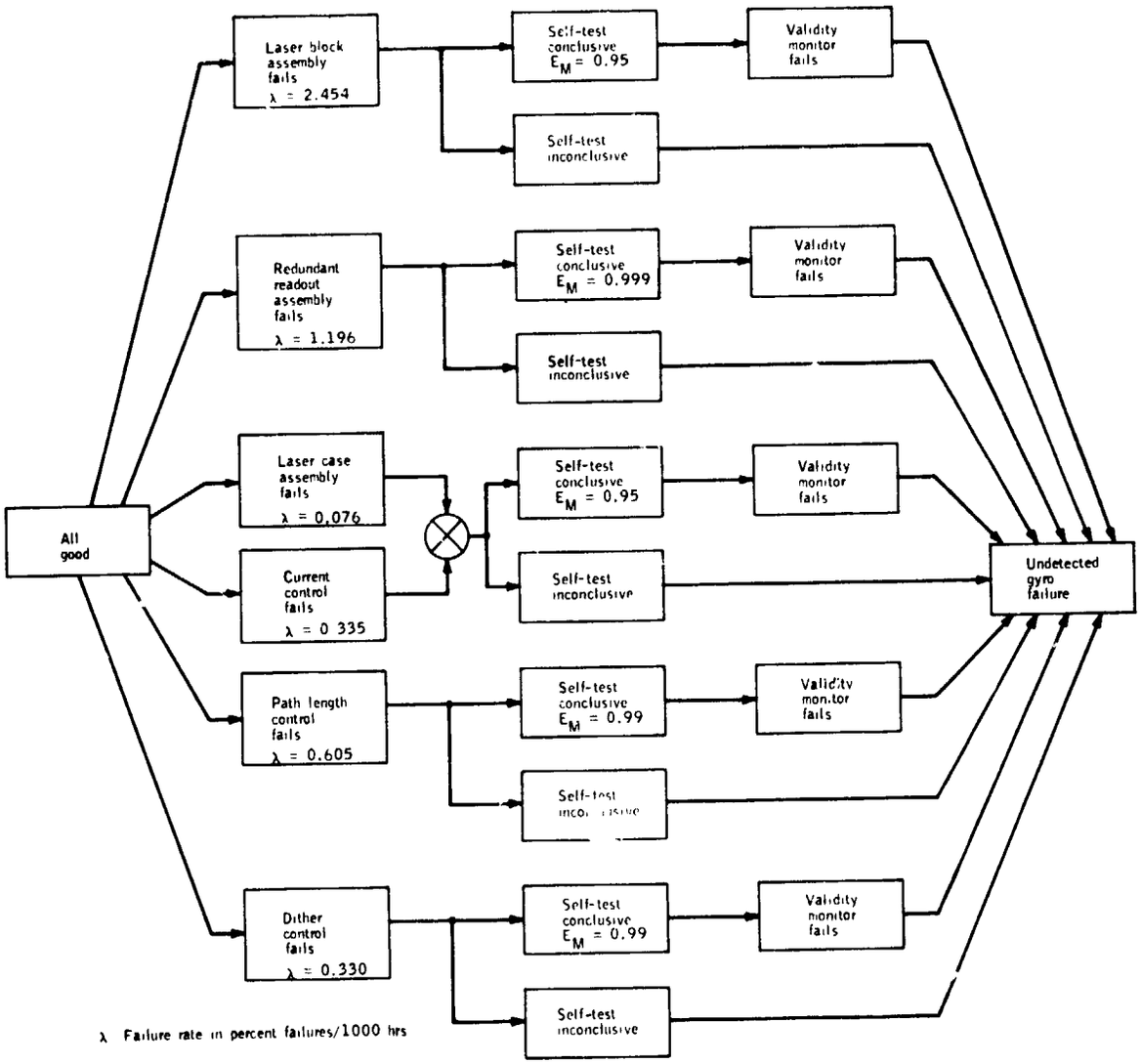


Figure 25. - Gyro failure model diagram

SECTION 5

SINGLE-CHANNEL COMPUTER FAILURE DETECTION AND ISOLATION

One of the basic mechanisms that makes strapdown inertial systems attractive is the ability to utilize the strapdown computer to time-share a number of different operations during a given computation cycle. This property also provides the system with a method to perform self-monitoring, since a portion of each computational cycle can be dedicated to verifying the proper operation of the system while the remaining portion of the cycle is used to perform the normal functional computations. Self-monitoring is performed to some degree on most digital systems to aid in fault isolation for maintenance. In this application, in-line monitoring or self-test is a key element in meeting reliability requirements.

To provide a high degree of fault detection and isolation (i.e., approaching 99 percent) with a self-monitored system, a concept using "selective redundancy" may be necessary. That is, any critical portions of the system that cannot continuously be self-tested must be redundantly mechanized and monitored. Continuous self-testing in a digital system implies periodic self-testing at a frequency sufficient to prevent a catastrophic system failure from occurring between tests. In the case of the flight control signals, a failure must be detected within milliseconds.

This section does not address the determination of criticality of functions or any tradeoffs involving alternate redundant configurations, but does assume critical functions will be redundant where necessary. For example, if a transmission line to another device is critical, sufficient parity/format checks will be incorporated or a dual line provided that can be comparison

monitored upon receipt by the device. This section primarily discusses in-line or self-monitoring techniques generally applicable to each channel of the dual-computer configurations. A qualitative evaluation of the self-test effectiveness is also provided so that the general feasibility of the approach can be evaluated against given system requirements.

Computer Definition

The tetrad computer consists of the following major functional elements: digital processor (CPU), memory, fault detection/reaction logic, input/output (I/O) control logic, and I/O functions. For this study, a Honeywell HDC-301-type general-purpose medium-speed digital processor is assumed. The CPU not only performs the necessary signal processing calculations but also controls all input/output via the I/O control logic. The intelligence necessary to direct the CPU is provided by the memory. The fault detection/reaction logic provides the fault reaction signal if a failure is detected and also acts as a detecting element for computer hardcore failures. Hardcore failures are those failures in the CPU, memory and I/O control that may prevent the failed computer from detecting its own failure.

The I/O control logic receives address and timing commands from the CPU, processes these commands through decoders, and provides output commands. These commands select the proper input or output signal to be processed and performs the multiplex switching and control for these signals. I/O functions contain the circuits to provide conversion of d-c, a-c, discrete and digital inputs and outputs. Figure 26 shows the general computer mechanization to be considered. Included in this diagram are the built-in test wrap-around signals that may be necessary for self-test.

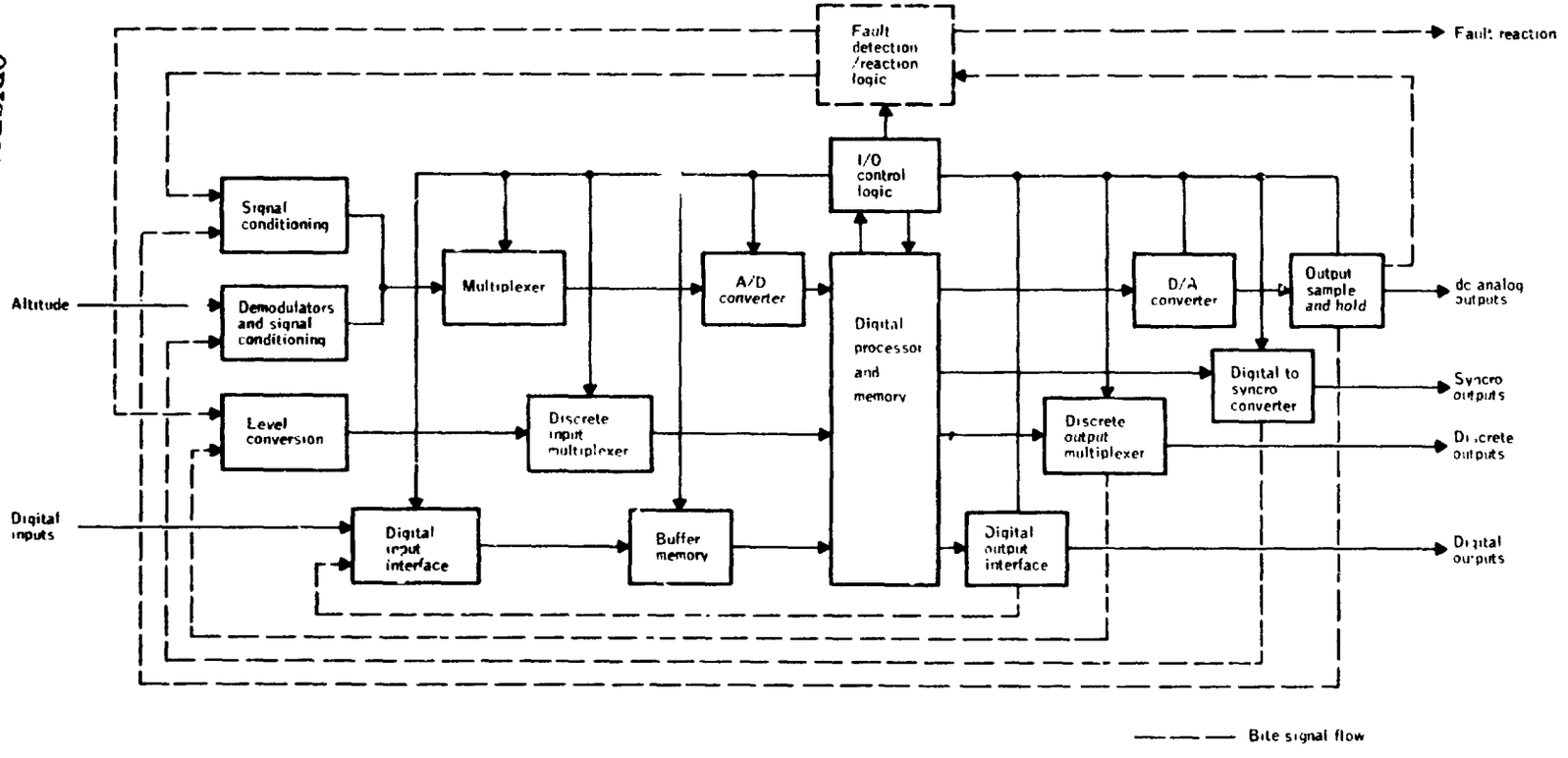


Figure 26. - Computer mechanization

Computer Failure Definitions

In the following discussion, six functional failure modes for the tetrad computer are defined. The major contributors to each mode are presented with a brief description of their impact on the failure mode. The six functional failure modes are: computer hardcore failures, memory failures, fault detection/reaction failures, CPU operational failures, multiplexed I/O failures and dedicated I/O failures.

Computer hardcore failures. - Computer hardcore failures are defined as those failures that will prevent the CPU and associated I/O from detecting its own failure and taking corrective action. Among these failures are those modes that result in a dead or inoperative/erratic computer. The major contributors to this failure mode are portions of the power supply, memory, I/O control and CPU.

An obvious contributor to computer hardcore failures is total loss of power. With no power, the CPU is incapable of performing any self-test. Less massive power losses can also cause hardcore failures such as partial loss of power to the CPU, I/O control, or fault reaction logic. These failures can cause the CPU to stop or render it incapable of communicating with its I/O. Massive memory failures will also prevent the CPU from performing useful self-test or taking corrective action. Among these failures are: dead memory, dead memory buffer control to the CPU, loss of addressing lines that prevent access to large blocks of memory, and inoperative instruction lines to CPU which scramble the CPU instructions. Many failures in the I/O control logic will prevent the CPU from reacting to known failures. Among these are any failure that prevents the CPU from communicating with the fault reaction logic.

Some CPU failures will also cause hardcore failures. Among these are the functions involving the program counter, addressing control and operation

code decoding. Failures in the program counter functions of the CPU will prevent it from performing proper instruction-fetch sequences and will result in erratic CPU operation. Failures in the addressing control functions will prevent the CPU from properly performing jump and branch instructions, and failures in the operating code decoding prevent the CPU from properly interpreting the instructions from memory, and, again, erratic operation will result.

Memory failures. - Memory failure modes other than the massive types described above are dependent on the type of memory and mechanization. The following general failure modes apply to most memory types: address control line failures, bite failures, bit failures. Address control line failures are those failures that either prevent access to a block of words or cause multiple access (more than one word in one fetch) to a block of words. These failures will result in a scrambled portion of data or instruction memory. The size of the failed blocks are dependent on memory mechanization but are typically 32 words or more. Bite failures are those failures that result in failures in portions of all words within a block. For instance, bits 1 through 4 of all words are inoperative. These failures are more common to semiconductor memories and are a result of inoperative memory chips. Bit failures include all those that result in any single bit in data or instruction memory failing. These failures will result in one bad instruction or data word.

Fault detection/reaction failures. - The fault detection/reaction functions are safety-critical portions of the computer. The fault-detection portion of these circuits are included to detect hardcore computer failures when the CPU and I/O are incapable of detecting failures in themselves. Because of the importance of these circuits to flight safety, an extensive failure modes and effects analysis is performed for each application. In general, these circuits are designed to be highly reliable, fail-safe and testable. The fault reaction portion of these circuits are also safety-critical, and again, extensive

failure modes and effects analysis is performed for each application. These circuits are also highly reliable fail-safe, and testable. Failure of these functions, along with any computer or sensor failure could result in an unsafe condition.

CPU operational failures. - CPU operational failures are those CPU failures which result in partial loss of CPU capability. Among these are: accumulator failures, I/O control failures, data register failures, adder carry failures, etc. These failures will result in improper operation on data or I/O devices. As a result, some or all computations performed by the CPU will be in error, even though the processor sequences properly through its instructions.

Multiplexed I/O failures. - Multiplexed I/O failures are failures in the control circuits that result in partial or complete loss of an I/O function. For example, if a switching chip analog input I/O should fail, an entire group of inputs would be inoperative. Similar failures exist for all I/O portions of the computer.

Dedicated I/O failures. - Dedicated I/C failures are failures that affect only one input or output. If these signals are safety-critical, they must either be testable or redundant.

Self-test Hierarchy

The computer control functions flow from the CPU to the I/O control and finally to the dedicated I/O. Because of this hierarchy of control, the following self-test approach is preferred:

- Ensure that the computer is capable of reacting to a failure within itself.

- Ensure that the memory is intact so that testing can be performed.
- Ensure that the CPU can properly process data and evaluate test results.
- Ensure that the CPU can control the I/O so that it can be tested.
- Ensure that the critical interfaces are operational.

If the computer is capable of reacting to a failure within itself, it can then be used to see that its memory is intact. Given these, the computer has the intelligence to perform testing functions. The CPU can now perform self-tests on itself to check its data processing capability. Given these functions, the CPU can be used to exercise the I/O circuits and evaluate their operation. The following subsection discusses various techniques that can be used to perform self-test on a digital computer system.

Computer Functional Test Descriptions

Monitoring and testing of the computer for hardcore failures is provided by circuits that do not require a functioning processor or memory to give failure warning. Typical systems will use one or more watch dog timers and possibly a dynamic computation monitor if detection in excess of 98% is needed.

Watch dog timer. - The purpose of the watch dog timer (WDT) is to protect against central processor or memory failures which prevent execution of a computation cycle in the prescribed period of time. It is designed to provide this protection without dependence on processor or memory functions. The essential element is a monostable single-shot flip-flop which

has a high output state for about 20% longer than the basic computation cycle after receiving an update pulse. A low output state disengages the DAFCS servos directly through hardware logic. To maintain system engagement, the DAFCS servos directly through hardware logic. To maintain system engagement, the DAFCS program checks that the WDT is not failed and then issues an output control pulse to update the flip-flop once every computation cycle.

Dynamic computation monitor. - The dynamic computation monitor (DCM) provides an independent and continous test of CPU capability to perform continous control functions. The concept defines a relatively precise control function which must be performed on an analog element by the CPU and I/O. The analog element to be controlled is an operational amplifier integrator. The objective of the control law contained in the software is to produce a stable ±5-vdc time-dependent triangular integrator output. The DCM control law also maintains certain similarities to the LINS computations.

- Exercises A/D and D/A conversion.
- Sample inputs and outputs a command at fixed rates.
- Exercises much of the instruction repertoire used by LINS computations.
- Relies on the real-time synchronism for maintenance of a precise computation interval.
- Uses CONSTANT and SPAD memory.

The integrator output is monitored by dedicated hardware for peak values both above and below nominal. Failure to exceed a 4.4-vdc magnitude at least every computation cycle causes disengage. Exceeding 5.6-vdc magnitude at any time also causes disengage.

Because the WDT or DCM do not require a functioning processor or memory to cause a disengagement, they are also relied upon for that function when failures are detected by other processor or memory monitors. In those cases, failure detection causes the computation flow to jump to a "fail loop" which prevents update of the WDT and DCM.

Memory tests. - Two basic memory testing schemes are in general use to test computer memories. These are parity and sum checks. In a simple single-bit parity scheme, each word sent to memory is routed through circuitry which first checks parity and then adds a "one" to the parity bit in each word if necessary to achieve odd parity. When any word is accessed, it is checked for correct parity by dedicated circuits, and, if an error is detected, a processor interrupt is immediately performed. Multiple-parity-bit schemes are available if additional checking is necessary. Among these are one parity bit per chip used to form a word and one parity bit for each bit in a chip to form a word. If two eight-bit chips were used to form a sixteen-bit word, the first multiple parity scheme would require two parity bits and the second eight parity bits.

Memory sum checks are used to protect against hardware failures in the memory, memory interface, or processor which cause actual or effective changes in the contents of critical instruction or data memory locations. A "critical" instruction or data is defined as one which can have significant effect, from a safety viewpoint, on the output signals.

The concept is to treat the contents of a given block of critical locations as data, and compute the sum of the contents of all locations in the block. This sum must then compare exactly with a precomputed check sum stored in data memory. Failure to compare, leads to failure warning via the CPU.

SPAD memory sum checks protect against failures in the memory, memory interface or processor which cause actual or effective changes in critical SPAD locations.

Since the contents of SPAD locations are variable, the following sum check concept can be used: Each critical SPAD variable is double stored; i.e., the A register contents are stored in both a primary and a secondary SPAD memory location. The primary location is used in computations on subsequent passes through the program. The secondary location is used only for sum checking. The sum check routine effectively adds the primary locations, subtracts the secondary locations and checks for a zero result. Failure warning is provided by the CPU if an error is detected.

Fault detection/reaction tests. - Because of the safety dependence on the fault detection/reaction circuits, a means of testing them is needed to ensure that no latent failures exist. These circuits are not normally tested continuously during flight because failure indications are usually latched to prevent transient resets. However, if the circuits are sufficiently fail-safe and reliable, a thorough automatic preflight is sufficient to provide safe operation. Testing usually consists of stim/measure and timing tests which check all components in the circuits. For instance, the watch dog timer is updated and then checked for not-time-out and timed-out at its minimum and maximum intervals.

CPU operational tests. - Monitoring of the operation of the central processor unit (CPU) is primarily performed by a set of special software. The basic CPU operation can be continuously tested in flight. The functions included in this test are:

- Data address lines of the CPU and memory
- Operation code decoding
- Information transfer to the A and B registers
- Logic instructions
- Shift and rotate instructions
- Load and store instructions

- Arithmetic instructions
- The accumulator
- Indexing
- Branch and return
- Conditional and unconditional jumps
- Special circuits

If a failure is detected by the CPU, a jump to a "fail loop" is executed.

Power supply tests. - The computer supplies which are critical to computer operations can be monitored by comparisons against nominals.

The purpose of these tests is two-fold:

- To compare the supply outputs against predetermined nominals and tolerances.
- Since these are known-value analog inputs, each of which can be wired to a different bank of the multiplexer, an inherent test of the analog I/O and analog-to-digital converter is performed.

Bite-the-tail tests. - All analog and discrete outputs are tested using a technique that has been labeled "bite-the-tail". Outputs are fed back to the input and re-entered into the processor through the appropriate input channel to be compared with the commanded output (to a suitable tolerance in the case of analog outputs). This type of test has the advantage of being an end-to-end check of the input/output since almost all of the circuitry is exercised by performing such a test.

Digital I/O tests. - Digital inputs and outputs are checked by means of a parity bit attached to each word at time of transmission and checked at time of receipt at the destination. This circuitry contains the multichannel digital interface.

Multichannel interfaces perform the following functions:

- Real-time synchronization between the redundant channels
- All data exchanges among the redundant channels
- Majority output or differential (digital) voting if desired

The real-time synchronization is necessary to ensure that all redundant channels are running the same problem so that their results can be compared. Data exchange is utilized primarily on inputs so that comparison of inputs can be performed prior to the computations. Because of comparisons within each computer, the interfaces are self-checking and no or little additional testing is necessary.

Dedicated input I/O tests. - The dedicated input I/O can be tested to some degree by providing stim signals from the computer to the input device. These tests usually require special dedicated hardware for each input to be tested. Continuous testing is usually not practical and therefore testing is limited to preflight only. Inflight tests are sometimes performed by using reasonable tests on the input signals.

Computer Failure Model

In an actual system application, a detailed failure modes and effects analysis is necessary to arrive at a detailed failure model. Included in a detailed model would be: programming restrictions to prevent use of not-tested CPU functions, the effects of redundant signal paths, restrictions on use of not-tested I/O control signals, and failure modes unique to the application and mechanization. A general computer model is shown in Figure 27.

Previously, it was stated that the fault detection/reaction logic should be designed to be highly reliable and failsafe. If this design is adequate, all failure paths containing these elements can be ignored when making the preliminary reliability calculations. The system failure state then reduces to the sum of probability of each failure mode occurring, multiplied by the self-test ineffectiveness.

Self-test effectiveness is dependent on the design, failure analysis, and failure testing effort. Numbers approaching 100% self-test are possible if considerable effort is made. This analysis and testing can easily become man years if a highly testable system (98+%) is required. The task consists primarily in defining all the possible safety-critical failure modes in the computer. In general, any failure mode that can be identified can be detected; but have all modes been defined? The parts count is high and it is especially difficult to identify all of the conditional failure modes. Also, latent failures are a potential problem.

Summary

Various proven techniques are available to achieve a reasonable self-test effectiveness. This effectiveness is largely dependent on the effort

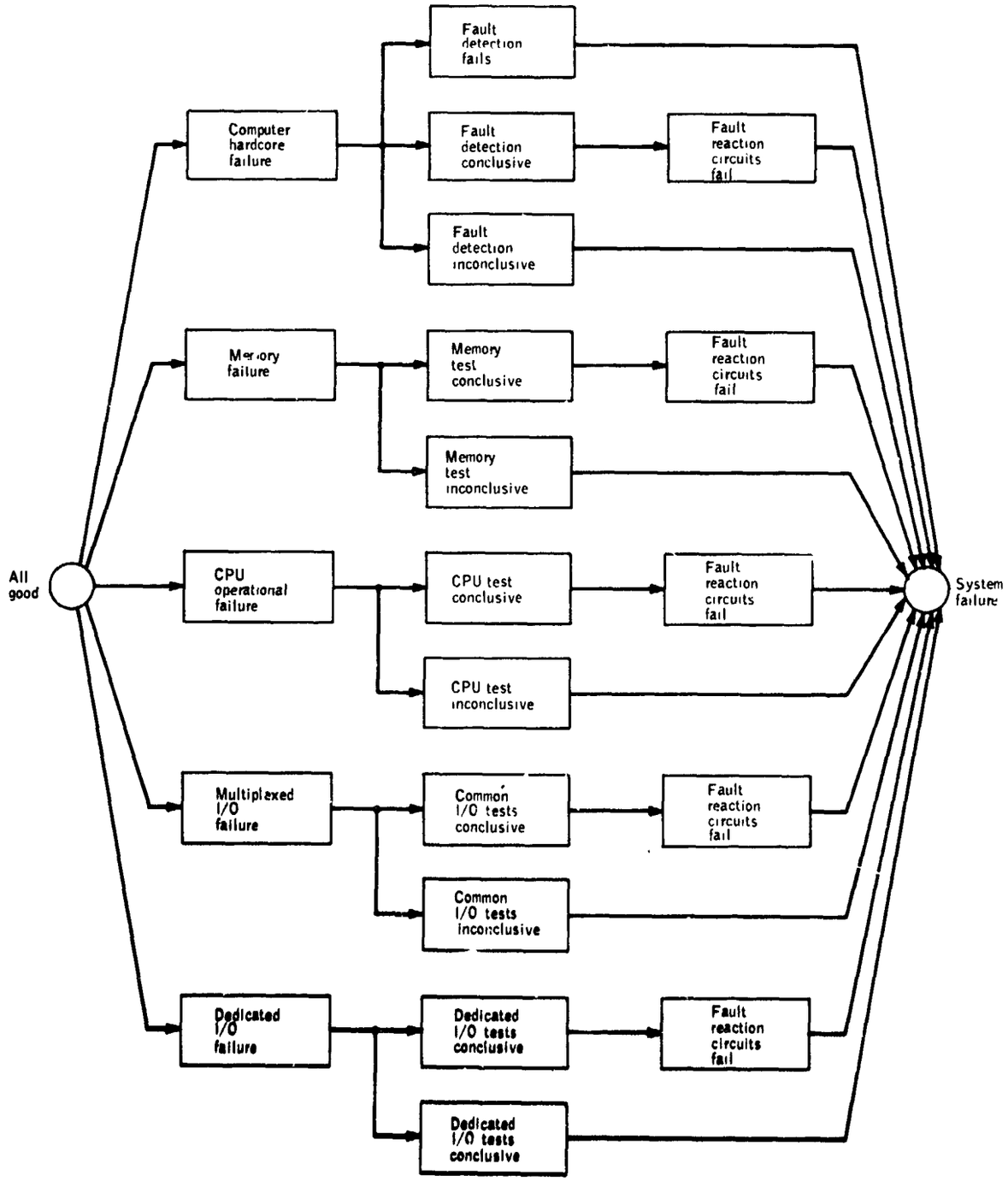


Figure 27. - Computer failure model diagram

spent on detailed failure modes and effects analyses and testing. To prevent unsafe conditions resulting from computer hardcore failures, some form of watch dog timer or dynamic computation monitor circuits is required. Also, selective redundancy may be necessary, particularly for critical I/O signals.

Table 5 summarizes the self-test hierarchy. Included are estimated failure rates and self-test effectiveness values. The values are estimated based on experience on similar systems and assume a failure modes and effects similar to conventional redundant systems. An overall self-test effectiveness of greater than 93 percent is reasonable for the tetrad computer, and this number can approach 100 percent given sufficient design and test effort. The dedicated I/O circuitry is typically the predominent contributor to the self-test ineffectiveness.

TABLE 5. - SELF-TEST HIERARCHY SUMMARY

Test type	Fault detection elements	Function	Estimated effectiveness	Estimated failure rate	Comments
Computer hardcore tests • CPU control • Memory control • I/O control	Fault detection circuits	Is the CPU capable of reaction to a detected failure?	99+%	3.7	Failure detection must be by external circuits if the CPU operation is unpredictable and is not capaole of detecting its own failure.
Memory tests • Parity • Sum checks	CPU	Is the memory intact?	98+%	4.5	Need to ensure that the self-test program is operational before using it for additional tests.
CPU operational tests • Accumulator • Data addressing • Arithmetic	CPU	Can the CPU properly process data?	98+%	2.0	All instructions are tested and worse-case but patterns are exercised and compared by CPU.
Multiplexed I/O tests	CPU	Can the CPU control the I/O?	97+%	6.5	Tests ensures that the multiplexed portions of the I/O are operational.
Dedicated I/O tests	CPU	Are critical interfaces operational?	75+% (as needed)	4.3	Test ensures that critical interfaces are operational.
Fault detection/reaction circuits test	CPU	Are the circuits fully operational?	99+%	-	Test typically performed at preflight only; ensures circuits used to detect computer hardcore failures are fully operational.

SECTION 6
IMPACT OF LASER GYRO FAILURE ON FLIGHT SAFETY

For flight occurring during IFR conditions, flight safety can be compromised by an undetected failure in any gyro which is part of a stability augmentation system, attitude reference system, or navigation system. The assumption is made that systems which provide a warning flag when they have failed (fail-safe) do not compromise flight safety in short haul aircraft because of backup systems of the same or different configurations. For instance, the inertial navigation system could be backed up by radio navigation (or vice-versa).

In a tetrad system, the first sensor failure can be detected at the system level with a confidence approaching 100%. Consequently, the system may be classified as a fail-safe system relative to the first sensor failure. Subsequent paragraphs discuss the rational for stating that individual gyro tests will identify the failed unit 96.5% of the time permitting the system to remain operational. However, an operational tetrad system with one gyro failure is no longer a fail-safe system 100% of the time, but is a fail-safe system (relative to a second gyro failure) 96.5% of the time.

Table 6 shows the effects of a failure in a functional area of the gyro. For instance, a failure of the laser case, laser block, laser readout or laser current control would make the gyro inoperative and its error would greatly exceed 360 deg/hr, which is typically the maximum error a stability augmentation system can tolerate even in a degraded mode. Consequently, all boxes associated with these areas are marked unusable (x). Loss of laser dither and laser path length results in gyro performance which is not usable for navigation but is usable (depending on the size of the error) for stability augmentation and attitude reference.

TABLE 6. - GYRO FAILURES VERSUS SYSTEM REQUIREMENTS

Failure	Failure type*	Stability augmentation gyro requirements, deg/hr			Attitude reference gyro requirements, deg/hr			Navigation gyro requirements, deg/hr		
		Unusable > 360	Degraded < 360 > 36	Full < 36	Unusable > 60	Degraded < 60 > 15	Full < 15	Unusable > .15	Degraded < .15 > .03	Full < .03
Laser case	NAS (> 360 deg/hr)	X	X	X	X	X	X	X	X	X
Laser block	NAS (>360 deg/hr)	X	X	X	X	X	X	X	X	X
Laser readout	NAS (>360 deg/hr)	X	X	X	X	X	X	X	X	X
Laser dither	NAS_D (<180 deg/hr)	Usable	X	X	X	X	X	X	X	X
Laser path length	N (< .5 deg/hr)	Usable	Usable	X	Usable	Usable	X	X	X	X
Laser current control	N (> 360 deg/hr)	X	X	X	X	X	X	X	X	X

*Failure types:

NAS = Gyro output unsuitable for navigation, attitude reference, and stability augmentation

NAS_D = Gyro output unsuitable for navigation and attitude reference but suitable for degraded stability augmentation

N = Gyro output unsuitable for navigation

X = Not usable

The undetected failure rate for a gyro in each of the referenced system is shown in Table 7. This is arrived at by multiplying the gyro failure rate and the self-test inconclusive factor. The gyro undetected failure rate is essentially the same for all three system functions, and the gyro undetected mean time between failure is in excess of 700,000 hours.

TABLE 7. - UNDETECTED FAILURE RATE

Failure	Failure rate, %/1000 hrs	Self-test inconclusive	Undetected failure rate, %/1000 hrs								
			Stability augmentation gyro requirements, deg/hr			Attitude reference gyro requirements, deg/hr			Navigation gyro requirements, deg/hr		
			Unusable >360	Degraded <360 >36	Full <36	Unusable >60	Degraded <60 >15	Full <15	Unusable >.15	Degraded <.15 >.03	Full <.03
Laser case (δ >360 deg/hr)	.076	.05	.0038	.0038	.0038	.0038	.0038	.0038	.0038	.0038	.0038
Laser block (δ >360 deg/hr)	2.4537	.05	.1227	.1227	.1227	.1227	.1227	.1227	.1227	.1227	.1227
Laser readout (δ >360 deg/hr)	1.196*	.001	.0012	.0012	.0012	.0012	.0012	.0012	.0012	.0012	.0012
Laser dither (δ <180 deg/hr)	.339	.01	.0033	- - -	- - -	.0033	.0033	.0033	.0033	.0033	.0033
Laser path length (δ <.5 deg/hr	.605	.01	- - -	- - -	- - -	- - -	- - -	- - -	.0060	.0060	.0060
Laser current control (δ >360 deg/hr)	.335	.01	.0034	.0034	.0034	.0034	.0034	.0034	.0034	.0034	.0034
Gyro failure rate 4.996 %/1000 hrs											
Gyro undetected failure rate, %/1000 hrs			.1344	.1311	.1311	.1344	.1344	.1344	.1404	.1404	.1404
Gyro undetected MTBF (1000's hrs)			748	765	765	748	748	748	715	715	715

* Redundant readout

100% per 1000 hrs = 1 failure in 1000 hours

δ = error

SECTION 7
CONCLUSIONS

The failure modes of laser gyros and computers were studied with respect to the potential use of a tetrad inertial navigation system in short-haul aircraft. This system was configured with two two-axis sensor channels, each channel containing its own computer. In this configuration, any set of sensor outputs can be used to derive the equivalent output of an orthogonal sensor triad.

The laser gyro was studied relative to the type of monitors necessary to isolate a gyro failure to a specific gyro within the tetrad system. In addition to the monitors, a redundant readout circuit in the gyro is considered necessary. The total potential effectiveness of the individual gyro monitoring circuitry is estimated at 96.5%. Note: Actual verification of this number requires a detailed failure mode and effects analysis with subsequent confirmation by actual hardware testing. An overall self-test effectiveness of 93% is reasonable for the computer and this number can approach the 99 to 100% range given sufficient design and test effort. The dedicated I/O circuitry is typically the predominant contributor to the self-test ineffectiveness.

The most promising system redundancy management concept consists of detecting the first sensor failure at the system level by analysis of the sensor outputs and by detecting the first computer error by comparison of computer outputs. Isolation of the first failure was found to be as good as the individual components (gyro and computer) failure detection capability.

For short-haul aircraft, flight safety is assumed to be compromised any time a system fails and a warning flag is not activated. In the tetrad system the first failure may be detected at the system level and a warning flag actuated with a confidence approaching 100%.

Isolation of the failure, in the case of the gyro and computers, can be accomplished 93 to 96% of the time, thus permitting the system to continue operating with one failure. However, a tetrad with one failure reverts to a system which is less than 100% fail-safe.

APPENDIX A
COMPUTER SYNCHRONIZATION

The computer hardware synchronization concept assumed for the study is shown in block diagram form in Figure A1. A 2-MHz oscillator in each computer is used to generate a 125-kHz ISA data transfer pulse rate signal, a 200-Hz data strobe ISA input cycle pulse, and a 40-msec (25-Hz) clock pulse. The 40-msec clock pulse is compared with the equivalent clock pulse from the other computer channel to derive a 40-msec sync pulse used to synchronize the computers, to reset and start the ISA input data timing counters (200-kHz and 125-kHz clocks), and to start the next 40-msec clock time count.

The 40-msec clock pulses are transferred between channels and subjected to the clock sync generator and failure detection logic shown in Figure A2. This logic generates a valid sync pulse when two pulses from the individual 40-msec clocks occur within a prescribed time interval (τ), which is derived from the 2-MHz oscillators, and reset each time a pulse is received. If the time difference between the occurrence of the first and second is greater than τ failure discrete F, is generated. In either case, a 40-msec clock sync pulse is generated that synchronizes the computers by releasing them from a "halt" condition entered at the end of each 25-Hz computation cycle. The derived 40-msec clock sync pulse also synchronizes the 125-kHz, 200-Hz ISA data transfer timing signals and resets/starts the 40-msec clock timer to generate the next 40-msec pulse.

The above operations occur simultaneously in each computer such that both become synchronized to the same 40-msec clock.

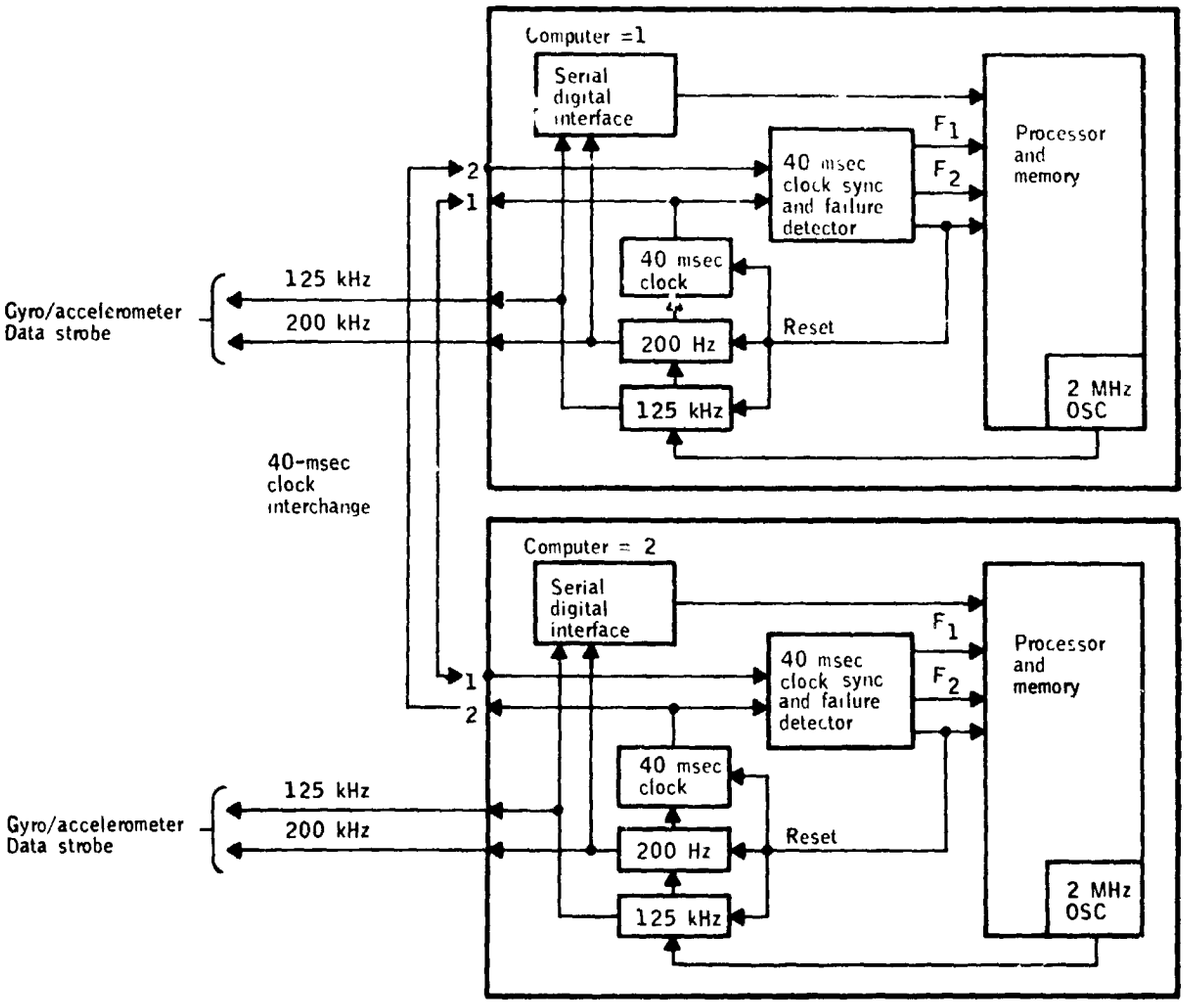


Figure A1. - Computer synchronization concept

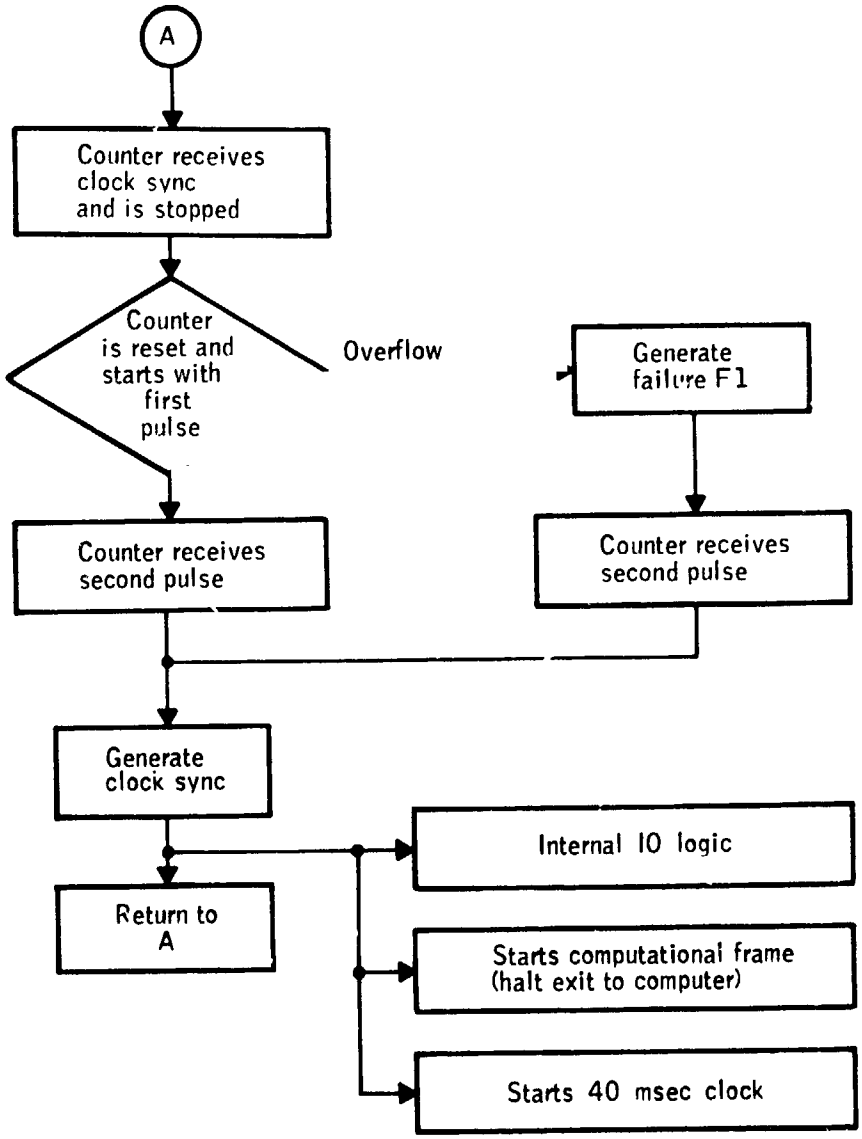


Figure A2. - Sync generator and failure detection logic

APPENDIX B
TETRAD SKEWED GYRO VOTING AND TRANSFORMATION EQUATIONS

The derivation of a typical set of error equations to be used in the gyro error detection/isolation routines for the tetrad system is described in this subsection. It is assumed that the two sets of orthogonal two-axis ISAs are placed such that each ISA has one input axis in the p and q (roll and pitch) plane, and the other axis rotated through an angle with respect to the p and q plane as shown in Figure B1. The p, q, and r (roll, pitch, yaw) coordiate frame was selected as the orthogonal reference triad. Figure B2 shows the projection of the tetrad input axes on the p and q plane.

The tetrad input axes can be expressed in terms of the reference triad and configuration geometry by inspection as

$$\begin{bmatrix} \omega_1 \\ \omega_2 \\ \omega_3 \\ \omega_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -C\alpha & S\alpha \\ C_B & S_B & 0 \\ C\alpha CA & -C\alpha SA & S\alpha \end{bmatrix} \begin{bmatrix} p \\ q \\ r \end{bmatrix}$$

where

ω_i = angular rate sensed by tetrad gyro
p, q, r = roll, pitch, yaw rates
α = 45°
B = 60°
A = 30°
C = Cosine
S = Sine

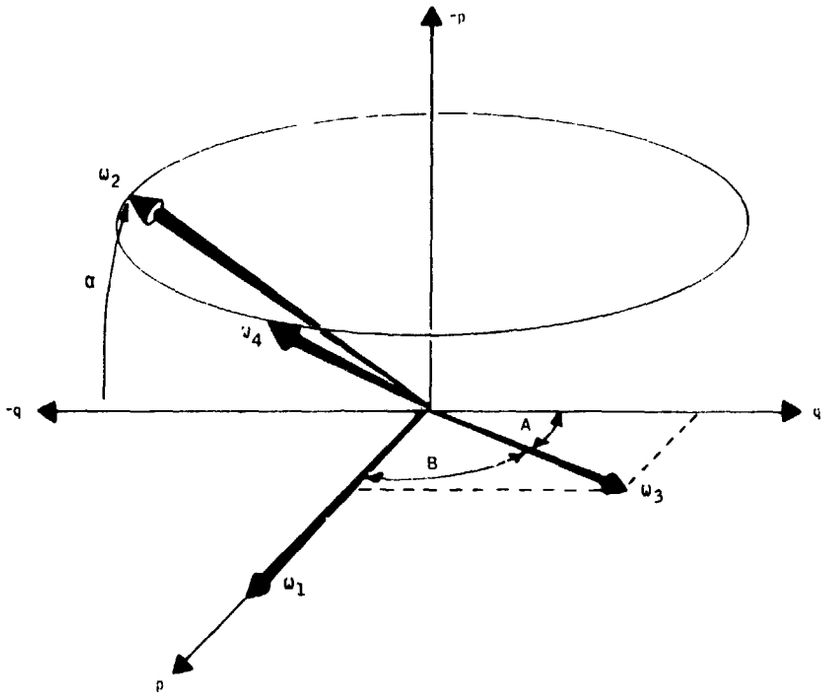


Figure B1. - Tetrad geometry

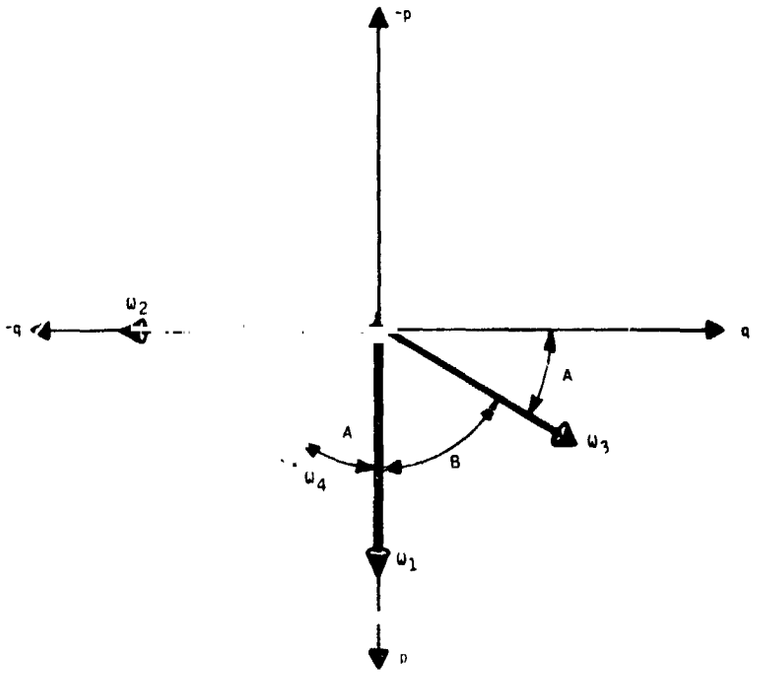


Figure B2. - Projection of hexad input axes into q-p plane

The two sets of orthonormal two-axis ISA outputs are defined by ω_1, ω_2, ω_3, and ω_4. The associated error equations are derived for the tetrad and are sufficient to detect a first failure.

The tetrad error equations are derived by selecting pairs of triads from the tetrad such as

$$\omega_i,\ \omega_2,\ \omega_3 \text{ and } \omega_1,\ \omega_3,\ \omega_4$$

and solving for p, q, and r in terms of the three-rowed submatrix inverses associated with each pair of triads. That is, for the selected pair of triads

$$\begin{bmatrix} \omega_1 \\ \omega_2 \\ \omega_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -C\alpha & -S\alpha \\ CB & SB & 0 \end{bmatrix} \begin{bmatrix} p \\ q \\ r \end{bmatrix}$$

$$\begin{bmatrix} \omega_1 \\ \omega_3 \\ \omega_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ CB & -C\alpha & -S\alpha \\ CAC\alpha & -SAC\alpha & S\alpha \end{bmatrix} \begin{bmatrix} p \\ q \\ r \end{bmatrix}$$

Taking the inverse

$$\begin{bmatrix} p \\ q \\ r \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ -CotB & 0 & Csc(B) \\ -Cot\alpha CotE & Csc\,\alpha & Cot\alpha Csc(B) \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \\ \omega_3 \end{bmatrix} \text{ and } \begin{bmatrix} p \\ q \\ r \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ -TanA & SecA & 0 \\ -Cot\alpha\, SecA & TanACot\alpha & Csc\alpha \end{bmatrix} \begin{bmatrix} \omega_1 \\ \omega_2 \\ \omega_4 \end{bmatrix}$$

In an ideal system, subtracting any two of the expressions for p, q, or r in each tetrad should yield gyro. Nonzero values are indications of gyro (ω_1) failures. The difference equations can, therefore, be identified as error equations used to evaluate tetrad functional integrity. Subtracting the terms for the tetrad yield the following equations:

$$E = CotA\ \ SecA\ (1-Sin\ A)\ (\omega_3 + \omega_1)\ [sc\alpha\ (\omega_2 - \omega_4)]$$

And for the angles as previously specified

$$E = 0.58\,(\omega_1 + \omega_3) + 0.707\,(\omega_2 - \omega_4)$$

To minimize the software requirements, the equation would be scaled such that one of the coefficients in each error equation would become unity.

To be capable of discriminating low-level (soft) failures from normal input random noise, the equation is first integrated and squared before comparison with an error tolerance equation for error detection. The error tolerance equations is a second-order polynomial and its coefficients represent statistical sensor output error tolerances. The tolerance equation is the form

$$T = A + Bt + Ct^2$$

where

A = constant, based on the covariance of the scale factor and misalignment calibration uncertainties input axis geometry, and worst case rates.

B = function of input axis geometry and random walk bias covariance.

C = function of input axis geometry and constant bias covariance.

If the inequality

$$E' = \left[\int_0^t E\,dt\right]^2 \mathrm{I}\; A + Bt + Ct^2$$

exists, a failure is indicated.

When a sensor failure is indicated, the appropriate error flag is set for use by the error response/action routine in the computer.

APPENDIX C
LASER GYRO READOUT CONFIGURATIONS

Establishment of criteria to determine the performance of the existing readout circuitry is difficult because the output is dependent on the input rate and may vary from zero pulses per second to several hundred thousand pulses per second.

The photosensor in the readout circuitry detects movement of the laser beam fringe pattern and converts this movement to a digital pulse train. The existing readout circuitry consists of two photosensors (1/4 wavelength of beat frequency apart). Each sensor generates a digital pulse train. The pulse trains are subsequently combined in a logic circuit to produce CW and CCW pulses depending on the direction on the laser beam fringe pattern is moving.

The two photosensor channels are not redundant in the normal sense; i.e., they do not produce the same pulse train when the fringe pattern is continually reversing direction but do produce a similar pulse train (90 degrees displaced with each other) when the fringe pattern is going in one direction.

There are four fringe pattern readout configurations, each employing a different number of photosensors, that are examined for potential applicability.

Configuration 1

The readout configuration shown in Figure C1 consists of a single photodetector and associated electronics feeding the line driver. Counts can be generated from this configuration, but the direction the fringe pattern is moving cannot be determined, so this configuration is of no practical value for this application but is shown as a building block for other configurations.

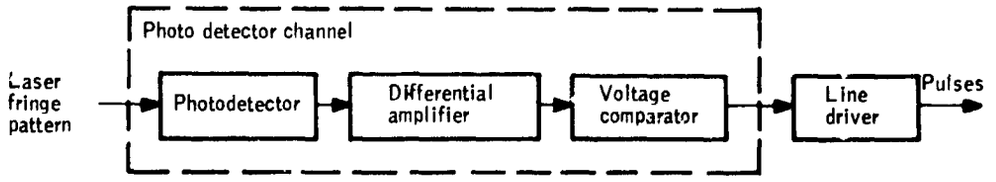


Figure C1. - Single-channel readout

Configuration 2

The readout circuitry used on the gyro is shown in Figure C2 and consists of two photodetector channels whose response to the moving fringe pattern is separated by 1/4 cycle of beat frequency). These two signals are processed by directional logic circuitry to produce CW and/or CCW pulses as inputs for the line drivers.

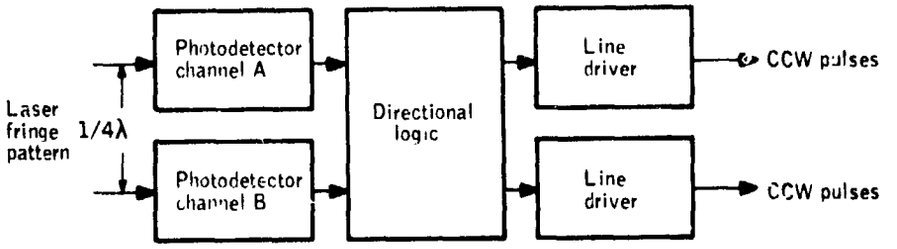


Figure C2. - Standard readout

Configuration 3

Figure C3 shows three photodetector channels being crossfed into three sets of directional logic and subsequently producing three comparable sets of CW and CCW pulses. Three angles are determined by subtracting the respective sets of clockwise pulses from counter-clockwise pulses for a given time period. Failure in the readout circuitry exists anytime the three angles are not within ±1 pulse of each other. It is not possible to have a failure in the readout circuitry and to determine which of the output angles are valid by examining the three output angles. For instance, a failure in the direction logic would result in two of the output angles being correct while a photodetector channel failure would invalidate two of the output angles.

Hard failures in the readout circuitry of Figure C3 may be detected using the following criteria:

- The three angles (A, B, and C) shall be ±1 pulse for each other.
- The summation of pulses $[\Sigma (P_{CW} - P_{CCW})]$ from any one of the outputs shall not equal zero.

Failure of the gyro to lase is also readily determined by this scheme as well as failure of any power supply related to the readout circuitry or lasing circuitry because the output pulse rate would go to zero.

Configuration 4

Figure C4 shows two separate sets of readout circuitry which are identical to the configuration 2 readout circuitry except that the photodetectors are physically adjusted so their response to the moving fringe pattern is separated by 1/4 cycle (1/4 λ).

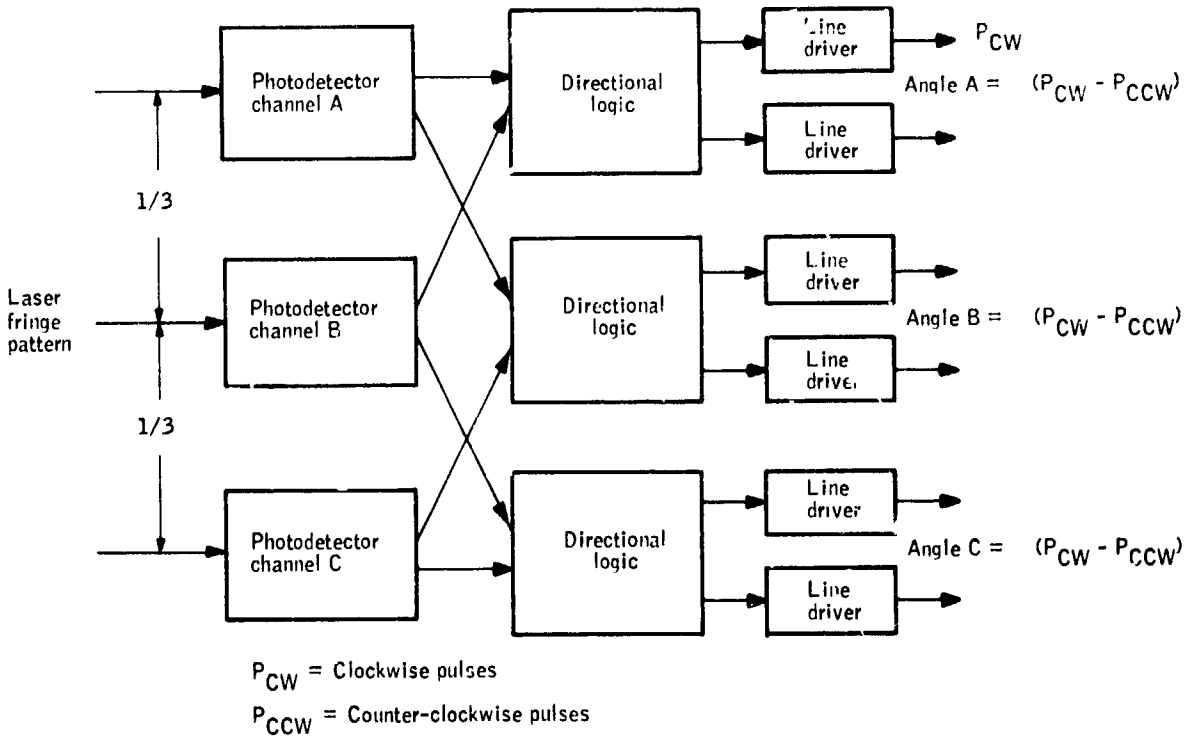


Figure C3. - Crossfed redundant readouts

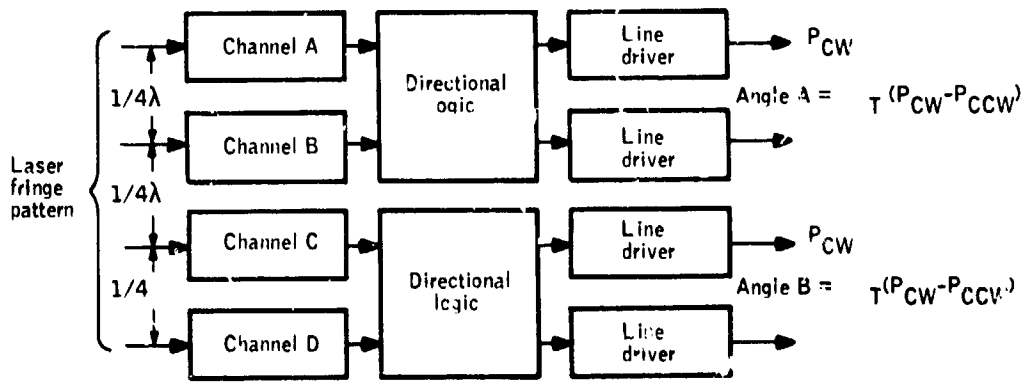


Figure C4. - Redundant readouts

Hard failures in the readout circuitry of Figure C4 may be detected using the following criteria:

- The two angles (A and B) shall be within ±1 pulse of each other.
- The summation of the pulses $[\Sigma (P_{CW} + P_{CCW})]$ from either of the outputs shall not equal zero.

Failure of the gyro to lase is also readily determined by this scheme as well as failure of any power supply related to the readout circuitry or lasing circuitry because the output pulse rate would go to zero.

Figure C5 is an input/output curve which illustrates the effect of dither spillover on pulse count. The amount of dither spillover is controlled by a physical alignment. Dither spillover is presently adjusted to be below ±1 count per cycle. For this scheme it would be adjusted between .5 counts/cycle and 1 count/cycle. For input rates near zero, the sum of the CW pulses and CCW pulses for a given time period $[\Sigma (P_{CW} + P_{CCW})]$ remain constant while the actual input rate is determined by subtracting the CCW pulses from the CW pulses for a given time period $[\Sigma (P_{CW} - P_{CCW})]$. This phenomenon is very useful in detecting failures inasmuch as zero pulses during a given time period does not mean zero rate but a failure.

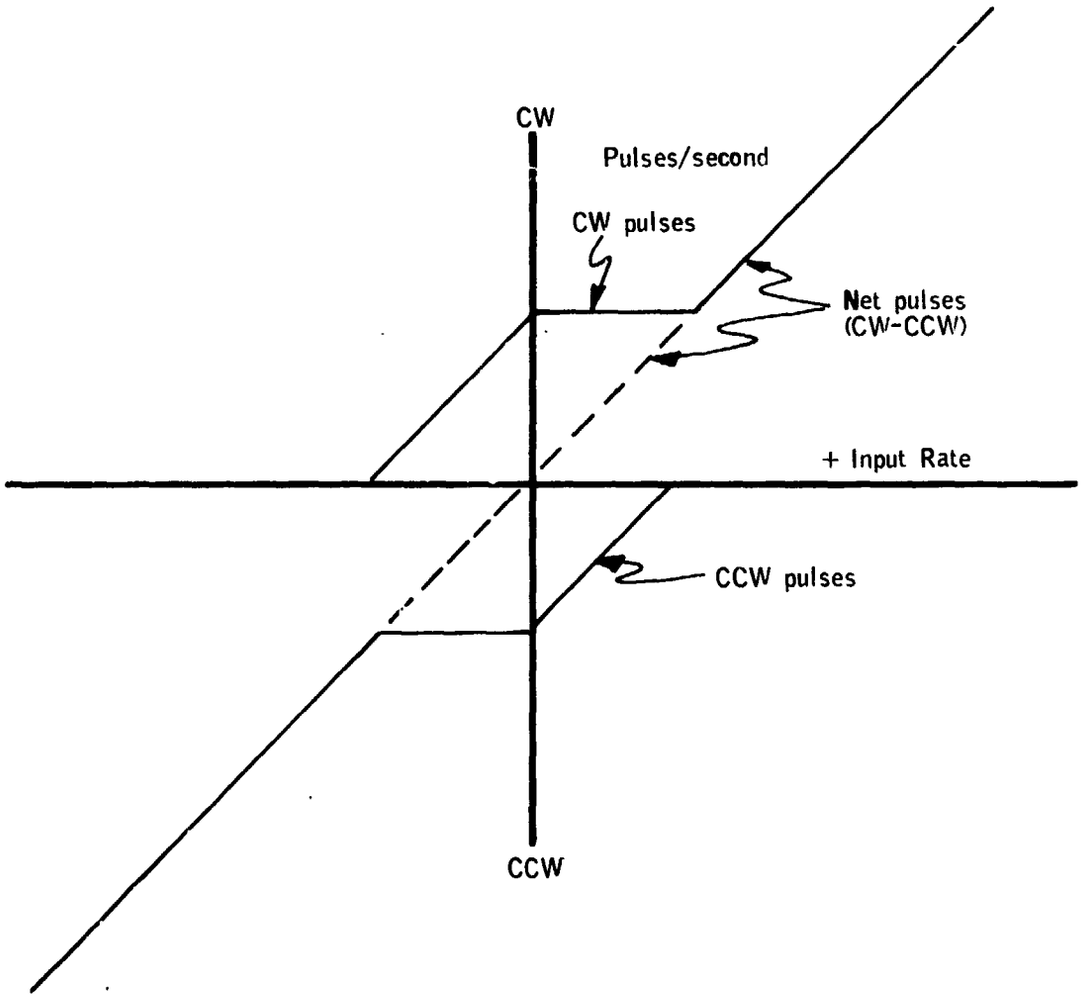
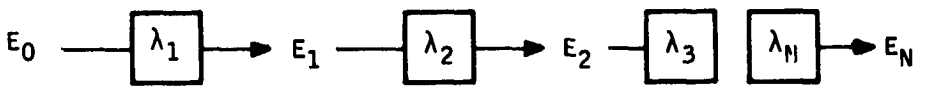


Figure C5. - Input/output curve (± count spillover)

APPENDIX D
FAILURE MODEL

In practical work it is often desirable to find an approximate solution to a problem that is in a simpler form and is easier to evaluate. We are all familiar with certain approximations, like x for sin x if x is small; the same approximation is also good for tan x under the same conditions. Let us derive the approximate solution for the state block diagram. The simplest way of obtaining an approximate expression is to use power series expansion for the given result and then to keep only the first few terms. If we tried to apply this method directly to our state block diagram model, we would have to obtain the solution in terms of exponential expressions and then expand these terms in power series using the proper expression for the given exponentials. It is obvious that the use of this procedure will be rather lengthy and time consuming. Let us investigate, therefore, an alternate approach.

In the simplest case the state diagram can be expressed as a sequence of arrows forming a straight path. An example of a general string is:



The state probability for the last state (failure state) will be given in Laplace transform by

$$P_N(s) = \frac{\lambda_1\lambda_2\lambda_3 \cdots \lambda_N}{(s+\lambda_1)(s+\lambda_2)(s+\lambda_3) \cdots (s+\lambda_N)s}$$

If we expand the denominator, we will obtain

$$s^{N+1} + s^N(\lambda_1 + \lambda_2 + \lambda_3 + \cdots \lambda_N) + s^{N-1}(\cdots\cdots) + \cdots\cdots$$

Substituting this expression in the equation giving $P_N(s)$ and then performing long division, we obtain

$$P_N(s) = \frac{\lambda_1\lambda_2\lambda_3 \cdots\cdots \lambda_N}{s^{N+1}}$$

$$\frac{\lambda_1\lambda_2\lambda_3 \cdots\cdots \lambda_N(\lambda_1 + \lambda_2 + \lambda_3 + \cdots\cdots + \lambda_N)}{s^{N+2}} + \cdots\cdots$$

The above expression is then inverted

$$P_N(t) = \frac{\lambda_1\lambda_2\lambda_3 \cdots\cdots \lambda_N t^N}{N!}$$

$$\frac{\lambda_1\lambda_2\lambda_3 \cdots\cdots \lambda_N(\lambda_1 + \lambda_2 + \lambda_3 \cdots\cdots + \lambda_N) + t^{N+1}}{(N+1)!}$$

If we use $\pi\lambda$ to denote the product of all failure rates and $\sum\lambda$ to denote the sum of all failure rates, we may rewrite the above formula as

$$P_N(t) = \frac{(\pi\lambda)t^N}{N!} - \frac{(\pi\lambda)(\sum\lambda)t^{N+1}}{(N+1)!} + \text{---- other terms}$$

Normally we will use only the first terms for the approximate expression giving the probability of failure. Thus

$$P_N(t) \cong \frac{(\pi\lambda)t^N}{N!}$$

Since, in this case, we are dealing with an alternating power series, the next term will give an indication of the error involved. Or, numerically

$$|\text{Error}| < \frac{(\pi\lambda)(\sum\lambda)t^{N+1}}{(N+1)!}$$

In addition to the λ's probabilities, self-test deficiencies can be added to the above expression. Where $C_N(s) = C_1 \cdot C_2 \cdot C_3$, etc., substitution into the above expression results in the composite approximate expression

$$P_N(t) \cong \frac{E_p (\pi\lambda C) t^N}{N!}$$

where

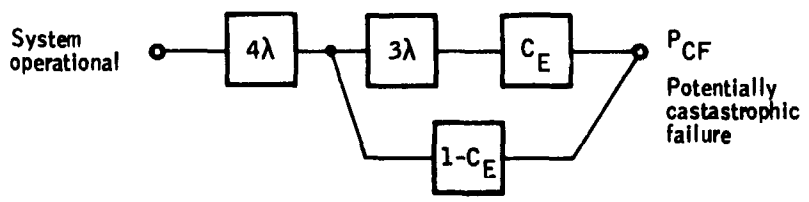
E_p is the sum of all paths from system operational to the point(s) of interest

N is the number of blocks in a path containing λ's

$\pi\lambda C$ denotes the products of all failure rates (λ's) and self-test deficiencies (C's) in a path

! denotes factorial

The following example demonstrates the use of this technique:



The probability of failure

$$P_{CF} = \frac{4\lambda \cdot 3\lambda \cdot C_E t^2}{2!} + \frac{4\lambda (1 - C_E) t}{1!}$$

which reduces to $6\lambda^2 C_E t^2 + 4\lambda (1 - C_E) t$.